(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号

特開平11－272594

(43)公開日　平成11年(1999)10月８日

(51)Int.Cl.[6]		識別記号	FI		
Ｇ０６Ｆ	13/00	３５４	Ｇ０６Ｆ	13/00	３５４Ｄ
	12/14	３２０		12/14	３２０Ｂ
	15/00	３３０		15/00	３３０Ａ
Ｇ０９Ｃ	1/00	６４０	Ｇ０９Ｃ	1/00	６４０Ｂ
		６６０			６６０Ｅ

審査請求　未請求　請求項の数44　ＯＬ　外国語出願　（全137頁）　最終頁に続く

(21)出願番号　特願平10－316819

(22)出願日　平成10年(1998)10月２日

(31)優先権主張番号　０８／９５７９８６

(32)優先日　1997年10月２日

(33)優先権主張国　米国（ＵＳ）

(31)優先権主張番号　０９／０５７９６６

(32)優先日　1998年４月９日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　597150049
タンブルウィード　ソフトウェア　コーポレイション
アメリカ合衆国　カリフォルニア州　94063　レッドウッド　シティー　ブロードウェイ　2000

(72)発明者　ジェフリー　シー　スミス
アメリカ合衆国　カリフォルニア州　94025　メンロ　パーク　アルトシュール　アベニュー　1305

(74)代理人　弁理士　中村　稔　（外７名）

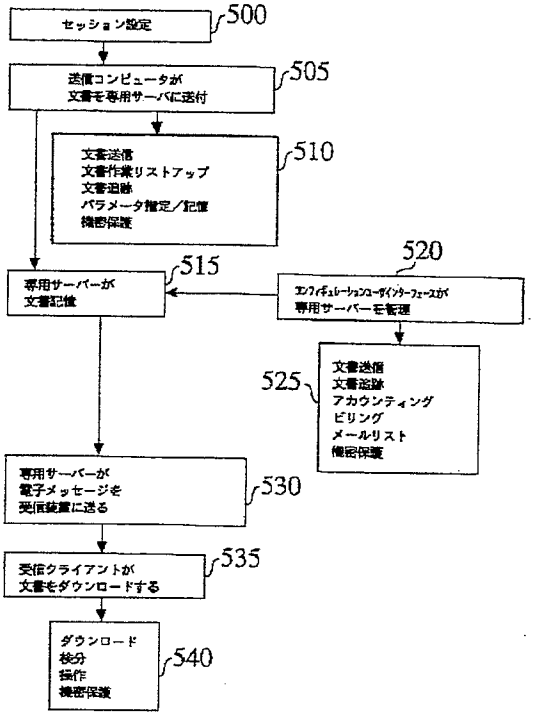
最終頁に続く

(54)【発明の名称】　電子ネットワーク上でのドキュメントデリバリ方法及び装置

(57)【要約】

【課題】　文書書式を維持しながら電子ネットワーク上で安全に文書送付する方法と装置を提供し、更に、システムへのアクセスを認められたユーザーだけに制限する機密保護を提供する。

【解決手段】　文書は、送信クライアントアプリケーションを使って送信コンピューターから専用サーバーへ送信され、専用サーバーは、文書を記憶し電子通知を受信装置に送り、文書は通知に応じて受信クライアントアプリケーションを使って専用サーバーからダウンロードされる。送信クライアントアプリケーションに依ってユーザーは、文書デリバリパラメーターを指定することができる。送信者操作証明登録システムとその使用方法も提供され、送信者は文書を暗号化し安全な方法で受信者に送信するために使用されるデジタル証明の生成を管理する。



1

【特許請求の範囲】

【請求項１】　セッションの間、電子ネットワーク上で送信コンピューターから単一パッケージとして少なくとも一つの文書を送付するための送信クライアントアプリケーションと、送信コンピューターからの前記少なくとも一つの文書を記憶し、電子メッセージを受信装置に送るための専用サーバーと、電子メッセージに応じて専用サーバーから前記少なくとも一つの記憶された文書をダウンロードし、見て、及び／又は操作するための前記受信装置上の受信クライアントアプリケーションとから成ることを特徴とする装置管理及びデリバリシステム。

【請求項２】　前記送信クライアントアプリケーションが、文書送付のパラメーターを指定するためのパッケージウインドウを更に含むことを特徴とする請求の範囲第１項に記載の装置。

【請求項３】　前記送信クライアントアプリケーションが、前記指定された文書デリバリパラメーターを構成可能に記憶するための記憶モジュールを更に含み、前記文書送付が前記記憶された文書デリバリパラメーターを使って開始されることを特徴とする請求の範囲第１項に記載の装置。

【請求項４】　前記送信クライアントアプリケーションが、前記送信コンピューター上でサポートされているアプリケーションからアドレスブックにアクセスするためのモジュールを更に含み、前記文書送付が前記アドレスブックの内容を使って開始されることを特徴とする請求の範囲第１項に記載の装置。

【請求項５】　前記文書が、前記文書を選択して、アプリケーションウインドウ、パッケージウインドウ、前記クライアントアプリケーションを表すアイコン、又は前記記憶された文書デリバリパラメーターにアクセスするためのアイコンの何れか一つの上にドラッグすることによって、送付されることを特徴とする請求の範囲第１項に記載の装置。

【請求項６】　前記コンフィギュレーションユーザーインターフェースが、前記文書を送信するための送信モジュールと、前記文書を追跡するためのトラッキングモジュールと、文書デリバリアカウントに関連する情報にアクセスするためのアカウントＣＵＩと、前記文書送付に関するビリングを管理するためのビリングモジュールと、メール配布リストを作成し管理するためのメールリストモジュールとから成ることを特徴とする請求の範囲第１４項に記載の装置。

【請求項７】　前記装置及び／又は前記文書へのアクセスを制限するための機密保護フレームワークを更に含み、前記機密保護フレームワークが、前記送信クライアントアプリケーション、前記受信クライアントアプリケーション、コンフィギュレーションユーザーインターフェースの内の少なくとも一つの中に少なくとも一つの機密保護モジュールを有することを特徴とする請求の範囲

2

第１項に記載の装置。

【請求項８】　前記機密保護フレームワークが、認証レイヤー、セキュアソケットレイヤー、パスワード保護、プライベートキー暗号化、パブリックキー暗号化、証明認証の内少なくとも一つをサポートしていることを特徴とする請求の範囲第１９項に記載の装置。

【請求項９】　専用サーバー上に記憶された少なくとも一つの文書を電子ネットワーク上にある通知受信装置に電子的に通知するための専用サーバーと、前記通知に応じて前記少なくとも一つの文書を受信するための前記電子ネットワーク上にある受信装置とから成り、前記受信装置が前記専用サーバーから前記文書をダウンロードするために受信クライアントアプリケーションを使用することを特徴とする電子ネットワークのための文書管理及びデリバリ装置。

【請求項１０】　前記受信装置が前記通知受信装置を含むことを特徴とする請求の範囲第９項に記載の装置。

【請求項１１】　ウエブブラウザ経由で前記専用サーバーを管理するためのコンピューターデスクトップ上のＨＴＭＬインターフェースを更に含むことを特徴とする請求の範囲第９項に記載の装置。

【請求項１２】　セッションの間、前記電子ネットワーク上で送信コンピューターの前記デスクトップから単一パッケージとして前記少なくとも一つの文書を送付するための送信クライアントアプリケーションを更に含むことを特徴とする請求の範囲第９項に記載の装置。

【請求項１３】　前記送信クライアントアプリケーションが、前記送信クライアントアプリケーションの主要な機能にアクセスするためのツールバーと、送信クライアントアプリケーションセッションの間に開始された全ての文書作業をリスト表示するためのパッケージマネージャーと、前記送信クライアントアプリケーションのための操作コマンドをリスト表示するメニューとから成る送信クライアントアプリケーションインターフェースを表示するためのアプリケーションウインドウと、前記文書送付のパラメーターを指定するためのパッケージウインドウと、前記文書送付が記憶された文書デリバリパラメーターを使って開始される、そのような、前記文書デリバリパラメーターを構成可能に記憶するための記憶モジュールとから成ることを特徴とする請求の範囲第１２項に記載の装置。

【請求項１４】　前記装置及び／或いは前記文書へのアクセスを制限する機密保護フレームワークを更に含むことを特徴とする請求の範囲第２４項に記載の装置。

【請求項１５】　送信クライアントアプリケーションを使用してセッションの間に電子ネットワーク上で送信コンピューターから専用サーバーへ単一パッケージとして少なくとも一つの文書を送付する段階と、前記専用サーバー上に前記送信コンピューターからの少なくとも一つの文書を記憶する段階と、電子メッセージを前記専用サ

ーバーから受信装置に送る段階と、電子メッセージに応じて前記受信装置上の受信クライアントアプリケーションを使って前記専用サーバーから少なくとも一つの記憶された文書をダウンロードする段階とを含むことを特徴とする電子ネットワーク上での文書管理とデリバリのための方法。

【請求項１６】　前記送信コンピューターデスクトップが、前記送信クライアントアプリケーションの主要な機能にアクセスするためのツールバーと、前記セッションの間に開始される全ての文書作業をリスト表示するためのパッケージマネージャーと、前記送信クライアントアプリケーションに関する操作コマンドをリスト表示するメニューとを有する送信クライアントアプリケーションインターフェースを持ったアプリケーションウインドウを表示する段階を更に含むことを特徴とする請求の範囲第１５項に記載の方法。

【請求項１７】　前記指定された文書デリバリパラメーターを記憶モジュール内に構成可能に記憶する段階を更に含み、且つ、前記文書送付が前記記憶された文書デリバリパラメーターを使って開始されることを特徴とする請求の範囲第４０項に記載の方法。

【請求項１８】　前記システムへのアクセスを制限するために、認証レイヤー、セキュアソケットレイヤー、パスワード保護、プライベートキー暗号化、パブリックキー暗号化、証明認証の内の少なくとも一つをサポートする機密保護フレームワークを提供する段階を更に含むことを特徴とする請求の範囲第１５項に記載の方法。

【請求項１９】　前記送信コンピューター上にサポートされたアプリケーションのアドレスブックの内容から前記文書送付を開始する段階を更に含むことを特徴とする請求の範囲第１５項に記載の方法。

【請求項２０】　コンピューターデスクトップ上で前記専用サーバーを管理するために、コンフィギュレーションユーザーインターフェースの主要な機能にアクセスするためのメインツールバーと、前記主要な機能内の機能にアクセスするための第二次ツールバーと、アクセスした機能との対話型インターフェースを表示するためのワークスペースと、前記コンフィギュレーションユーザーインターフェースに関する操作コマンドをリスト表示するメニューとを有するコンフィギュレーションユーザーインターフェースアプリケーションを表示する段階を含むことを特徴とする請求の範囲第１５項に記載の方法。

【請求項２１】　送信者が使用する送信コンピューターと、受信者が使用する受信コンピューターと、受信者情報を記憶するためのデータベースと、前記送信者が前記記憶された受信者情報に関する前記データベースを照会するための手段と、前記受信者から個人受信者情報を集めるための手段と、前記集められた個人受信者情報と前記記憶された受信者情報を比較するための手段と、前記受信コンピューターでパブリックキーとプライベートキーとから成るデジタル証明を制御可能に生成するための手段と、前記デジタル証明を記憶するための手段と、前記パブリックキーを前記送信コンピューターに送信する手段とから成ることを特徴とする、送信者が受信者のためにデジタル証明を生成するための装置。

【請求項２２】　前記送信コンピューターと前記受信コンピューターとの間に置かれるサーバーを更に含むことを特徴とする請求の範囲第２１項に記載の装置。

【請求項２３】　受信者情報を記憶するための前記データベースが前記サーバーにあることを特徴とする請求の範囲第２２項に記載の装置。

【請求項２４】　前記送信者が、前記記憶された受信者情報を前記データベースに照会するための前記手段が前記サーバーにあることを特徴とする請求の範囲第２２項に記載の装置。

【請求項２５】　前記受信者から個人受信者情報を集めるための前記手段が前記サーバーにあることを特徴とする請求の範囲第２２項に記載の装置。

【請求項２６】　前記集められた個人受信者情報と前記記憶された受信者情報を比較するための手段が前記サーバーにあることを特徴とする請求の範囲第２２項に記載の装置。

【請求項２７】　前記デジタル証明を記憶するための前記手段が前記サーバーにあることを特徴とする請求の範囲第２２項に記載の装置。

【請求項２８】　前記記憶された受信者情報と前記デジタル証明に関する送信者選択可能オプションとから成る証明要覧を更に含むことを特徴とする請求の範囲第２１項に記載の装置。

【請求項２９】　記憶された受信者情報に関するデータベースを照会する段階と、受信者から情報を集める段階と、前記集められた情報を前記照会され記憶された受信者情報と比較する段階と、前記比較を基にして前記受信者にソフトウエアを選択的に送信する段階と、前記ソフトウエアを使って前記受信者においてパブリックキーとプライベートキーとから成る前記デジタル証明を選択的に生成する段階とから成ることを特徴とする送信者が受信者のためにデジタル証明を生成するための方法。

【請求項３０】　前記デジタル証明のコピーを前記送信者に送信する段階を更に含むことを特徴とする請求の範囲第２９項に記載の方法。

【請求項３１】　前記パブリックキーのコピーを前記送信者に送信する段階を更に含むことを特徴とする請求の範囲第２９項に記載の方法。

【請求項３２】　受信者情報を記憶するための前記データベースがサーバーにあることを特徴とする請求の範囲第２９項に記載の方法。

【請求項３３】　前記データベースを照会する前記段階がサーバーによって実行されることを特徴とする請求の範囲第２９項に記載の方法。

5

【請求項３４】　前記受信者から情報を集める前記段階がサーバーによって実行されることを特徴とする請求の範囲第２９項に記載の方法。

【請求項３５】　前記集められた情報を前記照会され記憶された受信者情報と比較する前記段階がサーバーによって実行されることを特徴とする請求の範囲第２９項に記載の方法。

【請求項３６】　前記記憶された受信者情報と前記デジタル証明に関する送信者選択可能オプションから成る証明要覧を生成する段階を更に含むことを特徴とする請求の範囲第２９項に記載の方法。

【請求項３７】　送信者が使用する送信コンピューターと、受信者が使用する受信コンピューターと、受信者情報を記憶するためのデータベースと、前記受信者から情報を集めるための手段と、前記集められた情報と前記記憶された受信者情報が合致する場合、前記受信者のためにデジタル証明を制御可能に生成するための手段とから成ることを特徴とする、送信者が受信者のためににデジタル証明を制御可能に生成するための装置。

【請求項３８】　前記送信コンピューターと前記受信コンピューターとの間に置かれたサーバーを更に含むことを特徴とする請求の範囲第３７項に記載の装置。

【請求項３９】　受信者情報を記憶するための前記データベースが前記サーバーにあることを特徴とする請求の範囲第３８項に記載の装置。

【請求項４０】　前記受信者から情報を集めるための前記手段が前記サーバーにあることを特徴とする請求の範囲第３８項に記載の装置。

【請求項４１】　デジタル証明を制御可能に生成するための前記手段が前記サーバーにあることを特徴とする請求の範囲第３８項に記載の装置。

【請求項４２】　デジタル証明を制御可能に生成する前記手段が、前記サーバーから前記受信コンピューターへダウンロード可能なソフトウエアを含むことを特徴とする請求の範囲第３８項に記載の装置。

【請求項４３】　前記サーバーが前記デジタル証明を記憶するための手段を含むことを特徴とする請求の範囲第３８項に記載の装置。

【請求項４４】　前記記憶された受信者情報と前記デジタル証明に関する送信者選択可能オプションとから成る証明要覧を更に含むことを特徴とする請求の範囲第３７項に記載の装置。

【発明の詳細な説明】

【０００１】

【発明の背景】

【０００２】

【発明の属する技術分野】本発明は、電子ネットワーク上での通信に関する。より詳しくは、インターネットの様な電子ネットワーク上で、フォーマットされた文書を安全な方法で送付する方法と装置に関する。更に、本発明は、電子文書暗号化の分野に関する。より詳しくは、離れた受信者への電子文書の安全な送付についての技術に関する。

6

【０００３】

【従来の技術】インターネットやイントラネットの様な電子ネットワークは、様々なデータを記憶し配布するために益々使用されるようになってきている。例えば、ワールドワイドウエブ（ウエブ）ページには、テキスト、グラフ表示、ビデオ表示、アニメーション、音声を含めることができる。ウエブは、プラットフォーム、オペレイティングシステム、或いは電子メールシステムとは無関係に受信者が送信者から文書を受信することを可能にした。文書がコンピューターで受信されずファクシミリ機或いはインターネットに接続されたネットワーク化されたプリンターで受信される場合でさえもそのような通信は可能である。多くの場合、文書の送信者は、本文でイントラネットとよばれるローカルエリアネットワーク上に在る。送信者のコンピューターは、インターネットに直接接続されるか或いはイントラネットのサーバーを通して接続されている。直接インターネットに接続していないユーザーは、インターネットの場合にはインターネットサービスプロバイダ（ＩＳＰ）と呼ばれるアクセスプロバイダのサービスに加入する。

【０００４】ＩＳＰは、そのクライアントをインターネットに接続するネットワークを保守し、そのクライアントにホストとして作動するサーバーコンピューターを提供する。クライアントはモデム付きのコンピューターを使って公衆電話システムを通してＩＳＰに電話を掛け、インターネットにアクセスする。ＩＳＰはインターネット標準ＴＣＰ／ＩＰプロトコルを使って、クライアントが直接インターネットに通信するポイントツーポイント（シリアル）のリンクを通常提供する。現在存在する伝送の枠組みでは、例えばインターネット上で、ある種の文書を送信するのには適当でない場合が多々ある。重要な文書は完全な機密保護の下でで送信されなければならない。しかしながら、電子メールシステムの種類が違えば、機密保護支援のレベルも違う。それ故、電子通信が安全かどうか決定するのは難解或いは不可能である。

【０００５】電子通信に機密保護を提供するために、様々な暗号化スキームが使用されてきた。しかしながら、暗号化されたメッセージの受信者は、解読スキームを有するだけでなく、通信を解読するのに十分なハードウエアとソフトウエアを持っていなければならない。この様に、そのような暗号化されたメッセージを送信することは、しばしば現実的でなかったり不可能であったりする。この様に、ユーザーは文書を電子的に送信するのに気の進まないことが多い。これらユーザーは、遅くて費用の掛かるクーリエサービスや、従来の郵便サービスの方法に頼らざるを得ない。重要な或いは要注意の文書を追跡して、適切に受信されたと保証できることも望まれ

ている。しかしながら、電子ネットワークに沿って地点から地点へ文書を追跡することは、不可能でないにしても、大変難しい。例えば、インターネットを通じて送信される電子メールメッセージは、多くの別々のデータパケットに分割される。パケットは、インターネットを通じて宛先の受信者に別々に送信される。各々のパケットは、再度結合して元の文書を作り上げ受信者に渡す前に、異なるルートをとる。それ故その様な文書を追跡するには、インターネットの各々のリンクを通って各々の個々のパケットを追跡することが必要となる。

【０００６】加えて、コンピューターは受信された文書に、例えばパスワードや暗号文であるレベルの機密保護を提供することはできるが、電子通信は必ずしもコンピューターに向けられるとは限らない。この様に、プリンター或いはファクス機に電子的に送信される重要な文書は、公衆の目に晒される可能性がある。たとえその様な文書が安全に伝送されたとしても、受信された時点では判読できない場合もある。電子メールに共通する一つの問題点は、文書のフォーマットが失われることである。電子メールによって送信される文書は通常、電子メールメッセージ本体内のテキスト又はそれへの添付書類の何れかとして送信される。テキスト文書は通常、元の文書のフォーマットを維持しない。添付された文書は送信者と受信者の両方が互換性のあるソフトウエアアプリケーションを有する場合の様に、ある環境下ではフォーマットを維持できる。しかしながら、いくつかのフォーマットは、受信者が受信した文書を、作成されたのと同じアプリケーションを使って開く場合でさえ失われることがある。

【０００７】文書のフォーマットが変わるということは、深刻な問題を引き起こす。フォーマットが異なる場合、電子的フォームは互換性がない。間違ってフォーマットされた文書は、受信者には理解できない。多くのフォーマット変化が訂正可能である一方、時間と経費に関する受信者への負担は重大な問題である。それ故、インターネットの様な電子ネットワーク上で文書を安全に送付するための方法と装置を提供することは有益なことである。その様な方法と装置が文書の送信と受信を追跡できれば更に有益である。そのような方法と装置が送付された文書のフォーマットを維持できれば又更に有益である。例えばインターネットや他のオンライン発信源から提供されるコンピューター化された情報源の発達は、電子的に入手可能な情報の増大につながった。ネットワークを通しての情報と文書の安全な配布のために、機密保護が要望或いは要求され、情報を保護するため様々な設計と技術が開発されてきた。

【０００８】暗号化は、情報への招かざるアクセスを防ぐため情報ないし文書にスクランブルをかけるのに使用される基本技術である。図１は、シークレットキー暗号化１２１０ａのブロック線図であり、文書１２１２は、シークレットキー１２１４を使って、暗号化或いはスクランブル１２１６をかけられ、暗号化された文書１２２０になる。暗号化された文書１２２０は次に受信者に送信される。時に対称キー暗号方式と呼ばれる、シークレットキー暗号化は、招かざるアクセスを防ぐために独自シークレットキー１２１４を使って情報にスクランブルをかける技術を使用している。図２は、シークレットキー解読１２１０ｂのブロック線図であり、元の文書１２１２のコピーを復元するのに、暗号化された文書１２２０のスクランブル解除１２２２するため、同じ独自シークレットキー１２１４が必要となる。シークレットキー１２１４へのアクセスがなければ、暗号化された文書１２２０は、不当な干渉から安全に保たれる。

【０００９】シークレットキー暗号化１２１０ａと１２１０ｂに関する潜在的問題の一つはシークレットキー１２１４を安全に配布することへの挑戦である。例えば、送信者が文書１２１２を暗号化するためにシークレットキー暗号化を使用し、次に受信者に暗号化された文書１２２０を送信すると仮定する。受信者は、暗号化された文書１２２０を解読１２２２するためにシークレットキー１２１４を必要とする。シークレットキー１２２２が安全でないチャンネルで送信されると、機密保護の完全性が危険に晒される。多くのアプリケーションの場合、電話ないしファクスはシークレットキー１２１４送付の十分安全な方法を提供するが、一方、暗号化された文書１２２０は、ポスタ™　文書デリバリシステムを使ってインターネットで送付できる。しかしながら幾つかの例においては、送信者と受信者はシークレットキー１２１４の配布により強力かつ便利な手段を必要としている。

【００１０】パブリックキー暗号化は情報を安全に送付する、より強力、そして一般的により便利な手段を促進している。パブリックキー暗号化方法では、個々の受信者がパブリックキーとプライベートキーと呼ばれる一対のキーを所有する。キーペアーの所有者（受信者）は、パブリックキーを発行し、プライベートキーを秘密にしておく。図３はパブリックキー暗号化１２３０ａのブロック線図であり、文書１３１２は、パブリックキー１３３２を使用して、暗号化或いはスクランブルをかけられ１２３４、暗号化された文書１３３６になる。情報を受信者に送信するために、送信者は、情報を暗号化１２３４するために対象受信者の発行されたパブリックキー１３３２を使い、次に受信者は、情報を解読するために自分自身のプライベートキー１３３４（図４）を使う。従って、（情報を解読するのに必要な）プライベートキー１３３４は配布されない。図４はプライベートキー解読１２３０ｂのブロック線図であり、プライベートキー１３３４は、暗号化された文書１３３６のスクランブルを解除１２３８し、元の文書１３１２のコピーを復元するために必要とされる。プライベートキー１３３４へのアクセスがなければ、暗号化された文書１３３６は、不当

な干渉から安全に保たれる。

【００１１】パブリックキー暗号化１２３０ａと１２３０ｂは通常、パブリックキーとプライベートキー１３３２、１３３４の間の数理的関係を利用するが、これは、発行されるパブリックキー１３３２からプライベートキー１３３４を引き出すという危険性無しにパブリックキー１３３２の発行ができるようにする。パブリックキー暗号化アルゴリズムは一般に難解で、その結果多くのユーザーにとっては、時間が掛かり過ぎ実際の使用ができない。シークレットキー暗号化１２１０ａ、１２１０ｂは、パブリックキー暗号化１２３０ａ、１２３０ｂよりも一般にかなり早いが、シークレットキー１２１４を送信者から受信者へ送信する必要がある。ディジタル封筒システムにおいては、ユーザーはシークレットキー１２１４を使って文書１２１２を暗号化し、次に対象受信者のパブリックキー１３３２を使ってシークレットキー１２１４を暗号化する。暗号化された文書１２２０の受信者は、次にシークレットキー１２１４を解読するために自分のプライベートキー１２４０を使い、文書を解読するためにシークレットキー１２１４を使う。

【００１２】文書が送信中に変えられていないかを確認すること、或いは所定の文書の送受信者を確認することがしばしば役に立つ。細かなアルゴリズム（或いはメッセージ要覧）及びパブリックキー技術は、文書の完全性と伝送確認の解決策を促進している。デジタル証明は、暗号化された情報に対しより高い安全性を提供するためにも使用可能である。受信者が、パブリック／プライベートキーペアーを所有しており、パブリックキー１３３２を発行して、他の者が、受信者に送信される情報を暗号化するか、或いは受信者のデジタルサインを確認するかの何れかのためにパブリックキー１３３２を使用できる様にしたいと希望しているとする。受信者にとってパブリックキー１３３２を発行するのに安全な技術は、信頼できる機関にパブリックキー１３３２を登録することである。すると信頼できる機関は、特定のパブリックキー１３３２がその受信者に属していると証明できる。デジタル証明は、受信者ないし他の存在を特定のパブリックキー１３３２と結び付ける。

【００１３】後に開示する様に、デジタル証明は、パブリックキーと身元の記録であり、デジタルサインによって第三者により証明されたその二つの連合である。プライベートキーは、証明にはないが、ただ一つのプライベートキーが所定のパブリックキーと合致する。パブリック／プライベートキーペアーは、実際には次の特性を持つ一対の数字である。即ち、プライベートキーは、パブリックキーから安易に引き出せない。そしてパブリックキーは、プライベートキーを知ることによってのみ解読可能であるデータを暗号化するために使用することができる（ＲＳＡの様な幾つかのパブリックキーアルゴリズムは逆の特性も持っており、これをデジタルサインの使用に適する様にしている）。

【００１４】信頼できる、ないし証明する機関はデジタル証明を発行し保守する。開示されている先行技術システム及び方法論は、この様に文書の暗号化と安全な送付に関する方法を提供しているが、送信者によって実行され制御される簡単なデジタル証明生成と登録システムが提供できていない。その様なデジタル証明システムの発達は、主要な技術的進歩を作り出すであろう。

【００１５】

【発明の要約】本発明は電子ネットワーク上で文書を安全に送付するための方法と装置を提供する。本発明に依って、ユーザーは、一方で文書の元の書式を維持してながら、文書の送信と受信を追跡できるようになる。本文での論議の目的のために、「文書」という用語は、データストリーム、ビデオデータ、オーディオデータ、アニメーション、ＨＴＭＬ或いはＰＤＦ或いはエンボイ文書の様なプラットフォームに依存せずフォーマットされた文書、マイクロソフトワード或いはエクセル文書の様なプラットフォーム特定のフォーマットされた文書、テキスト文書の様なフォーマットされていない文書、特注作成されたレポート或いはウエブページ、ＳＱＬ記録の様な一つ或いはそれ以上のデータベース記録のグルーピングを始めとした、あらゆるデータの連続集合体を含むものとする。文書という用語は、一つ或いはそれ以上のその様な文書のグルーピングされたものも含む。本発明の好適実施例が、インターネット上での文書送信に利用できるようになっている一方で、本発明は同様に他の幅広い分野ないしローカルエリアネットワークにも適用可能である。

【００１６】本発明の本好適実施例に依ると、ユーザーが送信コンピューターのデスクトップから電子ネットワーク上で文書を送信可能な送信クライアントアプリケーションが提供されている。その様な文書は、文書作成アプリケーション内からも送信できる。専用サーバーが、送信コンピューターから受信された文書を記憶するために設けられている。すると、専用サーバーは、文書の送信を受信者に通知するために電子メッセージを受信装置に送る。対象受信者は、このメッセージに応じて専用サーバーから記憶された文書をダウンロードする。本発明の好適実施例では、受信装置はパーソナルコンピューターである。しかしながら代替例では、受信装置にはネットワークサーバー装置、ファクス機、プリンター、インターネット互換電話機、インターネットアクセス機器或いはパーソナルデジタルアシスタントが含まれる。

【００１７】受信装置に備えられている受信クライアントアプリケーションは、専用サーバーから文書をダウンロードするために使用される。受信クライアントアプリケーションは、ウエブブラウザであるのが望ましいが、文書書式を維持しながら記憶された文書を検索可能ないかなる他のソフトウエアアプリケーションであってもよ

い。受信クライアントアプリケーションに依って、受信者は文書を受信し、検分し、印刷し、操作することができる。送信クライアントアプリケーションは、アプリケーションウインドウを経てアクセスされる。アプリケーションウインドウは、送信コンピューターのデスクトップに表示される。アプリケーションウインドウには、主要機能にアクセスするための常駐のツールバーと送信クライアントアプリケーション用の操作コマンドをリスト表示するメニューとが含まれている。

【００１８】パッケージマネージャとパッケージウインドウも、アプリケーションウインドウからアクセスされる。パッケージマネージャーは、アプリケーションセッションの間に開始される全ての文書作業をリスト表示する。ユーザーは、パッケージウインドウに依って受信者、文書、送信オプションを含む文書送付のパラメーターを指定することができる。文書デリバリパラメーターは、後の変更及び／或いは使用のために記憶モジュールに記憶される。文書は、配布のためにいくつかの方法で指定される。ユーザーは、送信コンピューターデスクトップからアプリケーションウインドウ或いはパッケージウインドウの一つに文書をクリックアンドドラッグできる。文書は、送信クライアントアプリケーションを表すアイコン、又は記憶された文書のデリバリパラメーターにアクセスするためのアイコンの何れかにドラッグすることもできる。ユーザーは、更に、ローカル及びネットワークディレクトリを拾い読みし、希望の文書を選択できる。文書は、文書作成アプリケーション内からも送信できる。

【００１９】専用サーバーを直接呼び出しカスタマイズするために、コンフィギュレーションユーザーインターフェース（ＣＵＩ）が設けられている。本発明の好適実施例において、ＣＵＩはＨＴＭＬインターフェースである。それ故、専用サーバーはウエブブラウザ経由で直接呼び出されカスタマイズされる。このＨＴＭＬインターフェースは、文書の送信と追跡、アカウント情報へのアクセス、ビリングの管理、メール配布リストの管理のためのモジュールを含んでいる。ＣＵＩは、管理コンピューターデスクトップに表示されるＣＵＩアプリケーションウインドウ経由でアクセスされる。管理コンピューターは、送信コンピューター、受信コンピューター、専用サーバーないし電子ネットワークにおける他の存在であってよい。ＣＵＩアプリケーションウインドウは、主要機能にアクセスするためのメインツールバー及び第二機能にアクセスするための第二ツールバーを表示する。ＣＵＩアプリケーションウインドウは、アクセスされた機能への対話型インターフェースを表示するための作業場所と操作コマンドをリスト表示するメニューも含んでいる。

【００２０】本発明は更に、システムアクセスを認められたユーザーだけに制限する機密保護構造を提供する。サポートされる機密保護の型式には、認証レイヤー、セキュアソケットレイヤー、パスワード保護、プライベートキー暗号化、パブリックキー暗号化、証明認証が含まれる。機密保護構造は、一つ或いはそれ以上のモジュールとして提供することができ、送信クライアントアプリケーション、受信クライアントアプリケーション、ＣＵＩの少なくとも一つに組み込むことができる。送信者操作の証明登録システムとその使用方法が、提供されており、それによって送信者はデジタル証明の生成を制御し、文書を安全な方法で暗号化し受信者に送信するのに使用することができる。送信者は、以前に記憶された受信者情報を受信者から集められた情報と比較する。情報が合致する場合、送信者はキー生成ソフトウエアを受信者に送信し、それによりパブリック／プライベートキーペアーを含むデジタル証明を作成する。次に、送信者はパブリックキーを使用して文書を暗号化し受信者に送信し、そこで受信者は合致するプライベートキーを使用して文書を解読する。好適実施例において、サーバーは、送信者と受信者の間に配置され、システム機密保護、自動化、完全性のレベルを高める。

【００２１】

〔発明の詳細な説明〕本発明は、電子ネットワーク上で文書を安全に送付するための方法と装置を提供する。本発明は、ユーザーにそのような文書の送信と受信の追跡の可能性を提供する。送付の間、文書のフォーマットは維持される。本文での論議の目的のために、「文書」という用語は、データストリーム、ビデオデータ、オーディオデータ、アニメーション、ＨＴＭＬ或いはＰＤＦ或いはエンボイ文書の様なプラットフォームに依存せずフォーマットされた文書、マイクロソフトワード或いはエクセル文書の様なプラットフォーム特定のフォーマットされた文書、テキスト文書の様なフォーマットされていない文書、特注作成されたレポート或いはウエブページ、ＳＱＬ記録の様な一つ或いはそれ以上のデータベース記録のグルーピングを始めとした、あらゆるデータの連続集合体を含むものとする。文書という用語は、一つ或いはそれ以上のその様な文書のグルーピングされたものも含む。本発明の好適実施例は、インターネット上での文書送信に利用できるようになっている一方で、本発明は同様に他の幅広い分野ないしローカルエリアネットワークにも適用可能である。

【００２２】下文において述べる表示スクリーンとグラフィックユーザーインターフェースの構成は、本発明の本好適実施例に依って提供される。しかしながら、そのような表示スクリーンとグラフィックユーザーインターフェースは、本発明の代替実施例の要求に見合う様に簡単に変更修正されることは当業者には明らかである。下文における論議は、それ故、例示を目的として提供されており、本発明の範囲を制限するものではない。図５は本発明に依る文書送付システム１０の線図である。シス

テムに依って、ユーザーは、送信クライアントアプリケーション２０を使って電子ネットワーク１８上で、送信コンピューター１４のデスクトップ１２から文書１６或いは文書のセット、受信者アドレス或いは受信者アドレスのセットを送信できる。その様な文書は、ワードプロセッサー、スプレッドシートないしグラフィックアプリケーションの様な文書作成アプリケーション内からも送信することができる。送信クライアントアプリケーションは送信コンピューターに記憶されるのが望ましいが、送信コンピューターがアクセス可能な離れた場所に記憶されていてもよい。

【００２３】送信コンピューターは、専用サーバー２２接続する。専用サーバーは、例えば送受信者の間の文書送信を管理するためのインターネット基準の様な基準に従って機能する。専用サーバーは、インターネットサービスプロバイダ（ＩＳＰ）によって提供されるサーバー、或いは単独の専用サーバーであってもよい。本発明の好適実施例において、文書はハイパーテキストトランスファープロトコル（ＨＴＴＰ）を使って専用サーバーにアップロードされたりダウンロードされたりする。ＨＴＴＰは、ワールドワイド（「ウエブ」）上でサーバーに接続するために使用される通信プロトコルである。ＨＴＴＰの重要な有利な点は、それがアプリケーションでありプラットフォームに依存しないことである。この様に送受信者は同じウエブブラウザを使用する必要はなく、オペレイティングシステムでさえ同じものを使用する必要がない。

【００２４】専用サーバー２２は、送信コンピューター１４から受信した文書を記憶する。専用サーバーは、次に文書の送信の対象受信者に通知するために送信クライアントアプリケーションから受信したアドレスにある受信装置に電子メッセージを送る。この通知メッセージは、インターネットの簡単なメールトランスポートプロトコル（ＳＭＴＰ）を使ってテキスト（例えばＡＳＣＩＩ）メッセージとして送信される。本発明の好適実施例において、受信装置は、パーソナルコンピューター２４である。しかしながら、代替実施例においては、受信装置には、プリンター２６、ファックス機２８、ネットワークサーバー装置、インターネット互換電話機、インターネットアクセス器械、或いはパーソナルデジタルアシスタントが含まれる（図示せず）。

【００２５】通知メッセージは、文書のユニフォームリソースロケータ（ＵＲＬ）を含み、それによってサーバーは文書に位置を突きとめることができる。このメッセージに応じて、対象受信者は、受信クライアントアプリケーション３０を使って専用サーバー２２から記憶された文書をダウンロードする。受信クライアントアプリケーションは、受信装置に記憶されているのが好ましいが、受信装置がアクセス可能な離れた位置に記憶されてもよい。受信クライアントアプリケーションに依って受信者は、文書を受信、検分、印刷及び／或いは操作することができる。本発明の好適実施例において、受信クライアントアプリケーションは、ウエブブラウザである。この様に、対象受信者は、通知メッセージから直接ＵＲＬをコピーでき、それを受信コンピューターのウエブブラウザにペーストすることができる。ウエブブラウザは、次に専用サーバーから文書を検索する。本発明の代替実施例においては、受信クライアントアプリケーションは、文書書式を維持しながら、専用サーバーから記憶された文書を検索可能な全ての他のソフトウエアアプリケーションである。

【００２６】送信クライアントアプリケーションは、ＣＤ－ＲＯＭからコンピューターに、或いはウエブからダウンロードすることによって簡単にインストールされる。例えば、専用サーバープロバイダに既にアカウントを持つユーザーは、適切なアカウント情報で送信クライアントアプリケーションを作り上げることができる。そのようなアカウントを持たないユーザーは、アカウントを作るための情報を有するＵＲＬに導かれる。送信クライアントアプリケーションは、送信コンピューターのデスクトップに表示されるアプリケーションウインドウ経由でアクセスされる。一旦アカウント情報が適切に形成されると、アプリケーションウインドウが表示される。図６は本発明の好適実施例に依るアプリケーションウインドウ３２の画面である。

【００２７】アプリケーションウインドウの主要な機能は、送信クライアントアプリケーション作業の状態を見て、管理することである。アプリケーションウインドウは、送信クライアントアプリケーションの様々な機能とコンフィギュレーションユーザーインターフェースＣＵＩに連絡を取るための足掛かりとしても役立つ（下文にて論議）。本発明の好適実施例において、アプリケーションウインドウは、送信クライアントアプリケーションの主要機能にアクセスするためのメインツールバー３４を表示する。その機能の一つに、新しいパッケージ３６のための選択可能なボタンがある。新しいパッケージをクリックすると、新しいパッケージウインドウが開き（下文にて論議）、ユーザーが文書の配布を始められるようになる。オープンのボタン３８をクリックすると、セーブされたデリバリパラメーター又はセーブされたパッケージウインドウの何れかを開く（下文にて論議）。

【００２８】好適実施例では、メインツールバー３４は、ＣＵＩ機能へのインターネットショートカットであるボタンを含んでいる。そのようなボタンをクリックすると、ユーザーのウエブブラウザを立ち上げ、ＣＵＩにある適切なページを表示する。本発明の好適実施例では、この過程で、追加のログインは必要とされない。その様なボタンの例には、トラッキング４０、アカウント４２、ビリング４４及びメールリスト４６の各ボタンが含まれる。ボタンは、送信クライアントアプリケーショ

ン設定のために設けることもできる。例えば、セットアップボタン４８経由でアクセスされる選択ダイアログに依って、ユーザーは専用サーバーと代理サーバーアカウント情報を特定することができる。ユーザーは、全ての送信に関してデスクトップと専用サーバー間の接続を安全にするためのセキュアソケットレイヤー（ＳＳＬ）の様な低レベル安全通信プロトコルを使用するか否かを指定することもできる。

【００２９】送信クライアントアプリケーションは、サポートされたアプリケーションのローカルアドレスブックにアクセス可能である。本発明の好適実施例では、ユーザーがセットアップボタン４８を選択すると、本発明に依ってサポートされたアドレスブックをリスト表示するプルダウンメニューが提示される。ユーザーは、次に希望のアドレスブックファイルを選択する。停止ボタン５０は、専用サーバーへの全ての情報の送信を停止するために使用する。本発明の好適実施例では、一旦クリックすると、停止ボタンは押された状態のままとなる。送信を再開するには、ユーザーがボタンを再度クリックするとボタンは上がった位置に戻る。メニュー５２は、送信クライアントアプリケーション用の操作なコマンドをリスト表示する。本発明の好適実施例では、ファイルメニュー５４には、メインツールバー３４にあるボタンと同じ機能を有するコマンドが含まれている。その他のコマンドは送信クライアントアプリケーションに関する情報を提供するか、或いはＣＵＩの機能へのインターネットショートカットである。図６において、メニューは、編集５６、パッケージ５８、ＣＵＩ６０及びヘルプ６２をリスト表示する。

【００３０】アプリケーションウインドウは又、アプリケーションセッションの間に開始された全ての文書作業をリスト表示するパッケージマネージャー６４も表示する。パッケージマネージャーは、送信クライアントアプリケーションセッションの間に開始された全ての文書作業をリスト表示するアプリケーションウインドウ本体におけるエリアないしフィールドのセットである。送信クライアントアプリケーションが最初に立ち上げられると、パッケージマネージャーフィールドは空になる。しかしながら、文書が送信されるにつれて、それらはパッケージマネージャーにリスト表示される。図７は、本発明の好適実施例に依る文書作業７２を示すアプリケーションウインドウ３２の画面である。パッケージマネージャは、受信者６６、サブジェクト６８、送付の状態７０を表示する。配布中の状態は、アップロードが完了された動的パーセントテージとして表される。その他の可能な状態ラベルとしては「完了」、「エラー」、「ペンディング」、「ホールド中」が含まれている。

【００３１】文書は、処理順或いは処理順の逆に表示される。本発明の好適実施例では、現在処理中の文書７４は、太い文字で表示される。代替実施例では、最新の文書は、強調表示、点滅、色に依って示されるか、或いは印がされていないかである。リスト表示された文書７６をクリックすると、その項目を強調表示し、その文書を選択する。複数の文書も一度に選択できる。一旦文書が選択されると、ユーザーはメニュー５２を使用して、例えば文書をホールド、編集或いは削除することができる。ホールドは、ペンディング中の文書が処理されるのを防ぐ。文書は削除されるか或いはホールドが解除されるまで待ち行列に維持される。本発明の好適実施例では、リストにあるいかなる文書も、或いは全ての文書が削除可能である。現下の送信は完全に打ち切られ、既に処理された文書はウインドウから削除される。

【００３２】編集は、新しいパッケージウインドウ内で文書を開く（下文にて論議）。ユーザーは、次に文書を編集し、送信のために再度提出できる。文書が送信中に編集される場合、送信は打ち切られる。文書は、新しいパッケージウインドウで開かれ、次のペンディング中の文書が送信される。図８は、本発明の好適実施例に依るパッケージウインドウ７８の画面である。パッケージウインドウ７８に依って、ユーザーは文書送付のパラメーターを指定することができる。新しいパッケージウインドウは、例えばメニューないしツールバー選択によってアプリケーションウインドウからアクセスできる。パッケージウインドウはセーブされ、後で開かれる。更に、ユーザーが文書作成アプリケーションから送信クライアントアプリケーションへ文書を送信（印刷）する時点で、パッケージウインドウが開かれる。

【００３３】各々の文書送付処理には、送信者が、文書の受信者、送付される文書、デリバリオプションを指定する必要がある。その様なデリバリオプションには、優先順位８０、リクエスト確認８２、文書失効８６、予定通知８８、ビリングコード９０が含まれている。本発明の好適実施例は、クリアーフォーム９２、セーブフォーム９４、セーブパラメーター９６、送信９８の様な選択可能ボタンを含んでいる。所定の送付に関する受信者或いはメールリストの数がどれだけあっても、パッケージウインドウの「Ｔｏ：」フィールド１１０に指定される。各々の受信者は電子メールアドレス、別名、メールリストによって指定されなければならない。ユーザーは直接「Ｔｏ：」フィールドにアドレスを打ち込む。代わりに、ユーザーは「Ｔｏ：」ボタン１０８をクリックして受信者のウインドウにアクセスすることもできる。

【００３４】メッセージのサブジェクトは、サブジェクトフィールド１３４に入力される。メッセージ自体は、メッセージフィールド１３６に入力される。サブジェクト１３４とメッセージ１３６のフィールドは随意選択である。本発明の好適実施例では、サブジェクトは、電子メール通知メッセージとダウンロードされた文書に関するＨＴＭＬカバーページ上に現れる。メッセージは、電子メール通知にのみ現れる。パッケージウインドウにあ

る文書フィールド１１２に依って、ユーザーは、送付される文書がどんな数であっても指定することができる。文書は、幾つかの方法で指定される。ユーザーは、送信コンピューターデスクトップからアプリケーションウインドウ、パッケージウインドウの一つ、或いは送信クライアントアプリケーションを表すアイコン又は記憶された文書デリバリパラメーターにアクセスするためのアイコンの何れかに文書をクリックアンドドラッグできる。

【００３５】パッケージウインドウにある文書ボタン８４をクリックすると、送信者は、ローカル及びネットワークディレクトリを拾い読みし、希望の文書を選択できる。パッケージウインドウが文書作成アプリケーションから引き出されると、文書フィールドには自動的に現在使用中の文書が書き込まれる。ファイルフォーマットフィールド１３８に依って、ユーザーはどの電子フォーマットに文書がセーブされたか明記することができる。送信クライアントアプリケーションは、マックバイナリー、エンボイ、ＰＤＦ、ダイナドック、ＨＴＭＬの様な異なるフォーマットを容易にサポートできるようになっている。例えば、あるプラットフォームで操作可能なワープロアプリケーションで作成された文書は、異なるプラットフォームで操作可能な他のワープロアプリケーションのフォーマットでセーブすることができる。

【００３６】各々の配布処理は、関連した送信オプションを有する。本発明の好適実施例では、全てのオプションは、送付の前にユーザーが変更可能なディフォルト設定をされている。設定は、パッケージウインドウで見て、編集できる。優先順位フィールド８０において、ユーザーは、例えば、通常、低、高、至急の様な送付の優先順位を指定することができる。優先順位は、文書が専用サーバー同様クライアントに依って処理される順序も決定する。リクエスト確認フィールド８２は、受信者に、文書が首尾よく受信されたかどうかを確認する様に促すために使用される。リクエスト確認は、希望に応じて選択されたり或いはされなかったりする。機密保護ダイアログ１０１に依って、使用者は、高度な機密保護方法の様々なレベルを指定することができる。これらのレベルは、基本パスワード保護のためのパスワード１００を記すか或いはパスワード１０２の確認を要求することを含む。暗号化１０４或いは受信者に文書を受信するためにＳＳＬの使用を要求する１０６といった様な追加の機密保護の規定も提供できる。ユーザーが受信者にＳＳＬの使用を要求し、送信コンピューターデスクトップと専用サーバー間に安全な接続を使用しない場合、受信者は、専用サーバーへの接続を保護するか否かをたずねられる。

【００３７】文書失効フィールド８６に依って、ユーザーは、受信者が入手するためにどれだけの期間文書が専用サーバーに残るかを指定することができる。通知送信後１０日の様に、ディフォルトを設定してもよい。予定通知フィールド８８を使えば、ユーザーは、専用サーバーがユーザーに所定の送付を通知する予定時間と時刻を指定することができる。ビリングコードダイアログ９０を使えば、ユーザーは、ユーザーの送信クライアントアプリケーションアカウントに関連するリストから随意選択のビリングコードを選択できる。本発明の好適実施例では、ビリングコードの隠されたリストが利用可能である。リフレッシュボタン１１４は、専用サーバー上の最新のビリングコードリストを使ってリストをリフレッシュする。

【００３８】一旦ユーザーがパッケージウインドウにデリバリパラメーターを指定すると、ユーザーは、送信ボタン９８をクリックして文書送付を開始できる。受信者と文書フィールドの両方が正しく入力された場合のみ、送付は開始される。送信ボタンは、その様なフィールド両方が完成するまで作動しない。ユーザーがオフラインで作業中である場合、送信された文書は、接続が最終的に確立する時点で、送信のための待ち行列に入れられる。アドレスは先ず最新のローカルアドレスブックと比べられる。アドレスが合致しない場合、それらは、専用サーバーにその様にアップロードされる。専用サーバーは、次にアドレスをメールリストと合致させようとする。アドレスがなお合致しない場合、専用サーバーはアカウント所有者のドメイン名を追加する。

【００３９】部分的に完了したパッケージウインドウは、セーブフォームボタン９４を使ってキャンセル或いはセーブできる。セーブされたパッケージウインドウは後で使用するため再度開けることができる。セーブされたデリバリパラメーターは、セッションの間再生ベースで使用できる。パッケージウインドウから、ユーザーは、指定された送信オプション、アドレスリスト及び／或いは固定されたサブジェクト又はメッセージを含むデリバリパラメーターをセーブできる。デリバリパラメーターをセーブするには、ユーザーはセーブパラメーターボタン９６をクリックする。ダイアログボックスは、ユーザーにセーブするデリバリパラメーターに関する名称と場所を指定する様に促す。

【００４０】セーブされたデリバリパラメーターがアドレスリストを含む場合、ユーザーは文書アイコンをセーブされたデリバリパラメーターアイコン上にクリックアンドドラッグすることに依って送付を開始できる。文書は、送付に必要な残りの情報を提供し、送信が自動的に始まる。セーブされたデリバリパラメーターは、この様に受信者の特定のセットへの専用メールシュートとして機能する。現行の送信オプションは、送付を起こす前に変更修正或いは確認できる。全ての送信パラメーターを表示するウインドウが開けられ、ユーザーは、文書を送信する前にパラメーターを変更修正し、或いはメッセージを追加できる。本発明の好適実施例では、ユーザーは、パッケージウインドウを閉じる時に、送信オプショ

ン又は現行のアドレスリストに対する全ての変更をセーブする様促される。

【００４１】セーブされたデリバリパラメーターがアドレスを含んでいない場合、文書をセーブされたデリバリアイコンへクリックアンドドラッグすれば、パッケージウインドウが開く。セーブされた送信オプションと文書名がパッケージウインドウに記入される。文書が送信できるようにするには、ユーザーは受信者を指定しなければならない。セーブされたデリバリパラメーターは、関連するアイコンをクリックするか、或いは適切なメインツールバー３４又はメニュー項目を選択することによって開かれる。設定はパッケージウインドウに表示され、送付のために完了或いは変更修正される。送信クライアントアプリケーションが開いていない場合、セーブされたデリバリパラメーターを開くとパッケージウインドウだけでなくアプリケーションウインドウも開く。セーブされたデリバリパラメーターへの変更修正は、現行のセーブされたパラメーターを入れ替えるか、或いは違う名前の新しくセーブされたデリバリパラメーターを作成することによって保存される。

【００４２】セーブされていない変更がセーブされたデリバリパラメーターに対して行われた場合、ユーザーは、パッケージウインドウを閉じる際に変更をセーブする様に促される。送信者は、以前にアドレスリストを含んでいなかった現行のセーブされたデリバリパラメーターにアドレスリストを加えることができる。パッケージウインドウの設定は「ディフォルトとしての設定をセーブする」ボタン１１６を使ってセーブされる。図９は、本発明の好適実施例に依る受信者ウインドウの画面である。受信者ウインドウ１１８は、アドレスブック或いは以前定義されたメールリストから受信者の名前を選択するために使用される。本発明の好適実施例において、プルダウンメニュー１２０に依って、ユーザーは、ローカルアドレスブック或いはメールリストにあるアドレスにアクセスできる。例えば、プルダウンメニューにあるメールリストを選択し、リフレッシュボタン１２２をクリックすると、送信クライアントアプリケーションが構成されるアカウント用の専用サーバーに記憶されたメールリストの名前がリストボックス１２４に入ってくる。ローカルアドレスブックを選択し、リフレッシュボタンをクリックすると、選択ダイアログで指定されたアドレスブックからのアドレスがリストボックスに入ってくる。

【００４３】受信者のウインドウが開かれる度に、送信クライアントアプリケーションは以前に貯えられたアドレスのリストを表示する。リフレッシュをクリックすると、適切なソースからのリストを強制的にリフレッシュする。送信クライアントアプリケーションは、セッション内とセッション中の両方で次回の送信のために前回選択されたソースを提示する。キャンセルボタン１３５は、受信者のウインドウ表示をキャンセルする。ユーザーは、リストボックス１２４から項目を選択し、受信者としての選択を明記するために「Ｔｏ」矢印ボタン１２６をクリックする。本発明の好適実施例では、コントロールクリックは複数の項目の選択を可能にし、シフトクリックは項目の範囲を選択する。受信者は、受信者ボックス１２８に提示される。受信者ボックスリストにリスト表示された受信者は、削除ボタン１３０をクリックするか或いはキーボードバックスペースないしデリートキーを叩くことによって選択され、削除される。

【００４４】ユーザーが「ＯＫ」ボタン１３２をクリックすると、受信者ボックスリストにある項目が、パッケージウインドウ７８の「Ｔｏ：」フィールド１１０に表示される（図８参照）。本発明の好適実施例では、メールリストは、未決の場合接頭辞「リスト：」を有する。ユーザーは、パッケージウインドウの「Ｔｏ：」フィールドから受信者アドレスを更に削除或いは変更修正できる。指定された文書デリバリパラメーターは、後の変更修正及び／或いは使用のために記憶モジュールに記憶される。本発明の好適実施例では、送信クライアントアプリケーションとパッケージウインドウには、送信コンピューターのデスクトップからそれらを表すアイコン（図示せず）を選択することによってアクセスできる。

【００４５】コンフィギュレーションユーザーインターフェースは、専用サーバーを直接呼び出しカスタマイズするために提供されている。ＣＵＩは、管理コンピューターデスクトップに表示されるＣＵＩアプリケーションウインドウ経由でアクセスできる。代りに、ＣＵＩは、表をサポートする全てのウエブブラウザアプリケーションを通して、或いは送信クライアントアプリケーションを通してアクセスできる。図１０は、本発明の好適実施例に依るＣＵＩアプリケーションウインドウ１４０の画面である。本発明の好適実施例では、ＣＵＩは、ウエブブラウザ経由で専用サーバーを呼び出しカスタマイズするためのＨＴＭＬインターフェースである。このＨＴＭＬインターフェースは、文書送信、文書追跡、文書送付アカウントに関連する情報へのアクセス、文書送付に関するビリング管理、メール配布リストの管理のためのモジュールを含んでいる。

【００４６】ＣＵＩは、ユーザーと使用されるアカウントの型によって、異なる機能のセットを提供する。個々のアカウントホルダー、グループアカウントマンージャー、グループメンバーは、僅かに異なるインターフェースを見て、様々なセットのデータにアクセスし操作することができる。ユーザーがＣＵＩセッションを開始すると、アカウントの型が専用サーバーによって確認される。そして、特定のユーザーには、適切な機能とデータが提供される。本発明の好適実施例では、個々のアカウントホルダーとグループアカウントマネージャーは、全ての送付とアカウントに関連するアカウント情報へアクセスできる。アカウントマネージャーは、それ故アカウ

ントを使用する全てのグループメンバーの作業に関する情報へアクセスできる。

【００４７】アカウントマンージャーは更に、メンバーアカウントを作成及び管理することが認められている。グループメンバーは、メンバー自身の送付サービスに関する情報のみにアクセスできる。管理コンピューターは、送信コンピューター、受信コンピューター、専用サーバー、或いは電子ネットワーク内にある他のコンピューターであってもよい。ＣＵＩは、五つの主要機能即ち、新しいパッケージ１４２、トラッキング１４４、アカウント１４６、ビリング１４８、メールリスト１５０を含んでいる。本発明の好適実施例では、これら主要機能は、常駐のメインツールバー１５４にある選択可能ボタン１４２、１４４、１４６、１４８、１５０として表示されている。図１０において、このメインツールバーが水平方向に表示されており、クイットボタン１５２が更に含まれている。しかしながら代替実施例では、アプリケーションウインドウの構成は異なった形になっている。

【００４８】第二ツールバー１５６は、主要機能内にある第二次機能１６４にアクセスしナビゲイトするために提供されている。図１０において、第二ツールバーは、垂直方向に表示される。しかしながら、この構成は例示するためだけのものである。本発明では、メイン及び第二ツールバーを異なる方向に簡単に表示することができる。ＣＵＩアプリケーションウインドウ１４０に関する第二ツールバー１５６にある第二ナビゲーションは、アドレス１６６とオプション１６８を含む。全ての第二ツールバーに含まれるヘルプボタン１５８は、使われている機能に対するオンラインヘルプにアクセスするために使用される。ＣＵＩアプリケーションウインドウには、アクセスされた機能への対話型インターフェースを表示するためのワークスペース１６０も含まれている。メニュー１６２は、ＣＵＩに関する操作上のコマンドをリスト表示する。

【００４９】送信機能は、送信クライアントアプリケーションの機能を映す。送信機能は、新しいパッケージボタン１４２からアクセスされる。この送信機能に依って、ユーザーは、どのブラウザを使用しても離れた場所から文書を送信できる。送信機能に依って、文書は、送信クライアントアプリケーションによってサポートされていないプラットフォームからでも送信可能である。本発明の好適実施例では、セーブされているデリバリパラメーター、エンボイ変換、及びローカルアドレスブックへのアクセスは利用できない。送信機能にアクセスするために新しいパッケージボタンをクリックするとパッケージウインドウが出てくる。図１１は、本発明の好適実施例に依るＣＵＩパッケージウインドウ１７０の画面である。使用中の機能は、第二ツールバーにある項目１９２によって示される。

【００５０】所定の送付のために、ユーザーは、「Ｔｏ：」フィールド１７２に手動で名前を入力できる。メールリストも、プルダウンメニュー１７４から選択できる。ユーザーは、それによってメールリストを見て、操作する。本発明の好適実施例では、ユーザーは、ローカル電子メールアドレスブックへはアクセスできない。「Ｔｏ：」フィールド１７２に入力された項目が適切なドメイン書式を含んでいない場合（例えば「@」が落ちている）、項目はサーバーによってメールリストと比較される。項目がメールリストに無い場合、サーバーは、送信者のドメイン名を項目の最後に付け足す。送信者は、サブジェクトフィールド１７６とメッセージフィールド１７８にテキストを入力する。送信者は、「文書：」フィールド１８０に、文書の名前と、その文書へのパスををタイプすることによって送信される文書を指定する。代りに、文書は、ブラウズボタン１８２をクリックし、ローカル或いはネットワークディレクトリから文書を選択するために拾い読みして指定することもできる。

【００５１】複数の文書を送信するには、送信者は「文書を更に追加する．．．」リンク１８４をクリックする。次に送信者には、四つの追加「文書：」フィールドとブラウズボタンが追加された、新しいパッケージウインドウと同様のフォーマットを有するウインドウ（図示せず）が提示される。前のＣＵＩパッケージウインドウ１７０に既に入力されている情報は、新しいウインドウに繰り越される。この様に好適実施例では、送信者は文書を５つまで指定できる。代替実施例では、文書の数は幾つでも指定できる。リセットボタン１８６は、ウインドウにある全てのフィールドをそれらのディフォルト状態にクリアーする。送信ボタン１８８は、ディフォルトオプションを使って文書の送付を開始するために使用される。アドレスフォームに入力された情報が不完全或いは正しくない場合、本発明はエラーページ（図示せず）を送信者に表示する。それが認識されない場合、本発明は、送信者に文書の模写タイプを促す。模写タイプは、文書のフォーマットを指定し、文書を表示するための対応するアプリケーションを立ち上げるため受信者ブラウザによって使用される。好適実施例では、エラーページは直接編集され、新しい情報は直接提出される。送信が完了した場合、送信者に通知ページ（図示せず）が表示される。

【００５２】本発明の好適実施例では、ＣＵＩには、送信クライアントアプリケーションの送信オプションの殆どが含まれている（図８参照）。これらの送信オプションには、オプションボタン１９０をクリックして、ＣＵＩオプションページを開けばアクセスできる。図１２は、本発明の好適実施例に依るＣＵＩオプションページ１９４の画面である。その様なオプションには、優先順位１９６、リクエスト確認１９８、文書失効２００、予

定通知２０２が含まれている。しかしながら送信クライアントアプリケーションドライバーはサーバーからは利用できないため、文書タイプの様な特定の送信クライアントオプションは設けられていない。文書は、それ故文書の元の書式でのみ送信される。機密保護機能２０４は、本発明の好適実施例に組み込まれる。本発明の好適実施例は、米国で使用が現在の法の下で許可されている機密保護と暗号化特性をサポートする。本発明の代替実施例は、米国からの輸出を意図するソフトウエアアプリケーションに対するいかなる機密保護と暗号化の要件にも合致する。

【００５３】ＣＵＩユーザーは、受信者が文書にアクセスするために提供しなければならないパスワード２０６を指定することができる。ユーザーは、確認パスワード２０８、暗号化文書２１０を指定し、２１２を受信するのにＳＳＬを要求することもできる。パスワードは、サーバーで文書を暗号化するためのシークレットキーとして使用することができる。これは、文書がサーバーで記憶されるにも関わらずより高い機密保護レベルを提供する。暗号化文書機能２１０が選択されながらもユーザーがパスワードを特定しない場合、ＣＵＩは、ユーザーが設定の適用を試みる時点でエラーメッセージを送信する。ビリングコードオプション２１４に依って、ユーザーは、プルダウンメニューからの「無し」を含むビリングコードを選択できる。リストは、ＣＵＩのビリングモジュールで定義され保守される（図１９参照）。「ビリングコード」テキストリンクは、ユーザーをＣＵＩのビリングセクションに導く。ユーザーは、それによってビリングコードを見て、操作できる。

【００５４】リセットボタン２１６をクリックすると、ディフォルト設定状態に戻る。代りに、現在の設定をディフォルトとしてセーブ２１８することもできる。一旦オプションが設定されると、ユーザーは、更新ボタン２２０を使用してパッケージウインドウ１７０に戻る。送信ボタン１８８をクリックすると送付が開始される。追跡には、常駐のメインツールバー１５４にある追跡ボタン１４４からアクセス可能である。追跡サーチ機能は、アカウントから送信された送付についての情報に関してのＣＵＩデータベースを照会するために使用される。送信者は、それ故、受信者が特定の文書を受信したかどうかが分かる。データベースアーカイブは、過去の処理の記録に関してもサーチできる。図１３は、本発明の好適実施例に依るＣＵＩ追跡サーチページ２２２の画面である。第二ツールバー１５６からの第二ナビゲーションは、ログ２２４、サーチ２２５、レポート２２６、選択２２８、ヘルプ１５８を含んでいる。現在の機能１９２、サーチ２２５、は同一である。メインツールバーにある追跡ボタンは、デリバリログ（図示せず）としてアカウントから送信された全ての送付の記録を表示する。

【００５５】アカウントマネージャーは、グループアカウントから開始された全ての送付の追跡が可能である。グループメンバーは、メンバーによって個人的に開始された送付のみ追跡が可能である。デリバリログのフォーマットはトラッキング選択において指定される（図１４参照）。選択されたフォーマットは、デリバリログとトラッキングレポートの両方に利用される（図１５－１７参照）。本発明の好適実施例は、ユーザーが以前の或いはその後のログページにアクセスできる様にナビゲーションボタンを含んでいる。個々の送付に関する情報は、ログされた配布の総数の指示にと一緒にデリバリログに表示される。ログにある各々の項目のサブジェクトは、特定の送付に関するパッケージ詳細レポート（図示せず）にリンクしている。詳細レポートは、失効していなければ文書へのリンク、模写タイプ、メッセージを含む各々の送付の送信パラメーターを含んでいる。詳細レポートは、個々の受信者への送付の状態と処理に当てられた費用も含んでいる。ユーザーは、第二ツールバー１５６にあるログ２２４をクリックしてトップレベルログに戻ることができる。

【００５６】サーチ機能に依って、ユーザーは、特定の送付或いは送付のセットに関する情報と状態を正確に示すことができる。ユーザーは、関心のある送付を確認するためにサーチ基準のいずれかの組み合わせを指定する。複数の基準が指定された場合、サーチエンジンは、全ての基準の中で論理「ＡＮＤ」サーチを実行する。本発明の好適実施例において、サーチページグラフィカルユーザーインターフェース（ＧＵＩ）は、簡単にされている。共通のサーチ可能フィールドのショートリスト２３０は、サーチページに提示される。ショートリストには、五つのサーチ基準が含まれている。「Ｔｏ：」フィールド２３２に依って、ユーザーは、対象受信者のフルアドレス或いは受信者の部分電子メールアドレスを使ってサーチできる。部分電子メールアドレスにより、ユーザーはドメイン名を使ってサーチできる。

【００５７】「Ｆｒｏｍ：」フィールド２３４によって、アカウントマネージャーは、送付の開始者に依るサーチができる。アカウントマネージャは、プルダウンメニューからメンバーの電子メールアドレスを選択する。グループメンバーと個々のアカウントホルダーに対し、この所定のユーザーの電子メールが提供され、変更不可能である。「サブジェクト：」フィールド２３６によって、ユーザーは、文書のサブジェクトフィールドで見つけられるキーワードを入力できる。「文書：」フィールド２３８によって、ユーザーは、文書名でテキストサーチができる。ユーザーは、文書名で打ち込んだり、文書を選択するために文書リストを拾い読みしたりできる。

【００５８】「送信データ：」フィールド２４０によって、ユーザーは、特定の日又はその前後で送信された送付をサーチできる。サーチボタン２４２をクリックすると照会を開始し、照会に合致する全ての送付のレポート

を戻す。リセットボタン２４６をクリックすると、フォームをクリアーしてディフォルト設定にする。ショートフォームの下部にある「更なるオプション．．．」ボタン２４８をクリックすると、ユーザーは、ショートリストからの全てのフィールドを含む、サーチ可能なフィールドの第二、拡張リスト（図示せず）を有するページに導かれる。好適実施例では、拡張リスト内の追加フィールドには次のものが含まれる。ビリングコード：フィールドによって、ユーザーはプルダウンメニューにある予め定義されたリストから選択できる。

【００５９】「配布状態：」フィールドによって、ユーザーは、送付状態のメニューから選択できる。送付状態オプションには、全ての受信されたもの、されていないもの（通知失敗のもの及びピックアップされていないものの両方を含む）、確認されたもの、されていないもの、ペンディング通知及び失敗通知が含まれる。ユーザーは、文書失効、予定通知日、受信日付、メッセージフィールドをサーチすることもできる。サーチ結果は、追跡レポートに表示される。追跡レポートは、追跡選択ダイアログに記されたフォーマットで表として表示される。図１４は、本発明の好適実施例に依るＣＵＩ追跡レポート選択ダイアログ２５０の画面である。ダイアログによって、ユーザーは、文書フォーマット２５２を選択したり或いは新しいフォーマット２５４を定義したりできる。本発明の好適実施例では、ユーザーは、二つの予めフォーマットされたレポート、即ち基本フォーマット、ビリングコードフォーマットから選択できる。要約と詳細情報レポートの両方が、各フォーマットで利用できる。

【００６０】ダイアログによって、ユーザーは、ページ毎の行数２５６を指定することができる。加えて、ユーザーは、受信者要約情報２５８、又は詳細情報２６０を示すかどうかを選択する。更新２６２をクリックすると全ての変更がセーブされ、ユーザーは、追跡レポートにアクセスした元のレポート或いはページに戻る。ユーザーがレポートに戻ると、新しい選択設定で表示される。ダイアログはリセットボタン２６４を使ってリセットされる。図１５は、本発明の好適実施例に依る基本フォーマット２６６での受信者要約追跡レポートの画面である。サーチ結果が表示されると、第二ツールバー１５６にある第二ナビゲーションは、送信者がレポートモード２２６に在ると示す。追跡レポートの要素と動きは、デリバリログのそれらと一致する。

【００６１】本発明の好適実施例では、送付は日付によって分類され、入力順の逆に表示される。しかしながら、代替例において、送付は、例えば受信者によって、入力順に表示或いは分類される。送付項目の次のページは、ネクストボタン２８４をクリックしてアクセスされる。受信者要約追跡レポートは、「受信者：」フィールド２７０に、特別の送付の第一受信者の名前２６８のみ、或いは送付が送信されたメールリストにある第一受信者をリスト表示する。リストにそれ以上の名前がある場合、表示（．．．）が、名前の次に出る。送付の受信者数が、「受信済み：」フィールド２７２にリスト表示され、通知された数が「通知済み：」フィールド２７４にリスト表示される。この情報は全ての受信者に渡って総計される２７６。

【００６２】例えば、図１５に示される最も最近の送付は、「サブジェクト：」フィールド２７８にリスト表示されたパーティー招待である。パーティー招待が送信された日付は、「送信：」フィールド２８０に示されている様に１９９７年１月２２日である。追跡レポートは、総計三つのパーティー招待文書が送信されたことを示す。全ての三人の受信者が通知され文書を受信している。第一受信者２６８“ｊａｎｅ@ｉｓｐ．ｃｏｍ，”のみが「受信者：」フィールド２７０に表示されている。図１６は、本発明の好適実施例に依る基本フォーマットでの受信者詳細追跡レポートの画面である。受信者詳細追跡レポート２８２は、「受信者：」フィールド２７０に個々の送付の個々の受信者をリスト表示する。「受信済み：」２７２フィールド及び「通知済み：」２７４フィールドは、個々の受信者が送付を通知され、送付を受信した特定日をリスト表示する。例えば、図１６は、パーティー招待の三人の受信者、彼等の通知と受信日を別々にリスト表示している。

【００６３】受信者詳細追跡レポートは又、全てのメールリストを拡張する。本発明の好適実施例では、メールリストは、処理された送付に関して拡張されているだけである。先の予定送付と進行中の送付は、その様に示される。図１７は、本発明の好適実施例に依るビリングコードフォーマット２８６での受信者詳細追跡レポートの画面である。ビリングコードフォーマットは、ビリングコード２８８を表示し、ビリングコードと日付により結果を分類する。ＣＵＩアカウント管理機能は、「アカウント」１４６と表示してあるメインツールバーボタンから利用可能である。アカウント機能は、グループアカウントマネージャー、個別アカウントホルダー、メンバーアカウントホルダーの様なアカウントのタイプ及びユーザーのタイプによって変化する。サーバーソフトウエアはユーザーのアカウントタイプを確認し、適切な機能と利用可能な情報を作成する。

【００６４】全てのユーザーは、アカウントバランスを含む個々のユーザーのアカウントに関する記録にある管理アカウント情報を見ることができ、そのパスワードを変更することもできる。しかしながら、グループアカウントマネージャーは拡張された能力を有し、グループメンバーの新しいアカウントを作成できるだけでなく、そのアカウント情報を編集できる。この様に、グループアカウントマネージャーに表示された第二ツールバーの第二ナビゲーションは、情報：３０２、メンバー検分：３

０４、メンバー追加：３０６の様な機能を含んでいる（参照図１８）。情報ページ（図示せず）は、専用サーバーに記憶されたグループアカウントに関する基本情報を表示する。その様な基本アカウント情報には次のものが含まれる。

【００６５】・アカウント名
・アカウントタイプ
・作成日付
・最新アクセス日付
・最大許可されたメンバーの数に対する現在のメンバーの数

アカウントマネージャーは、メンバーページ（図示せず）経由で現在のメンバーリストを見て、管理できる。アカウントホルダー情報には次のものが含まれる。
・マネージャー名
・電子メールアドレス
・会社名
・アドレス

基本アカウント情報とアカウントマネージャー情報は編集できない。

【００６６】グループアカウントパスワードは、情報ページから変更できる。マネージャーは、現行のパスワードと希望の新しいパスワードを入力し、新しいパスワードを確認しなければならない。マネージャーは、更新をクリックして新しいパスワードを提示する。好適実施例では、情報ページは、パスワードが最後に何時変更されたかをマネージャーに知らせるフィールドも含んでいる。パスワードが一度も変更されていない場合、このフィールドはアカウントの作成日付を表示する。アカウントの変更を認められたサーバーマネージャーに、リンクを提供することもできる。マネージャーは、情報ページにあるメンバーテキストリンクをクリックし、或いは第二ツールバー１５６の検分メンバー機能を選択することによってメンバーのリストを見ることができる。図１８は、本発明の好適実施例に依るグループアカウントマネージャーアカウント検分メンバーウインドウ２８８の画面である。ある実施例では、マネージャーは、自分が、フォーマット、ページ毎の行数、検分メンバー表の分類順序を指定することができるプリファランス（図示せず）へのリンクを使用する。

【００６７】検分メンバーページは、グループアカウントの名前２９０と総数から表示されたメンバー数２９２を表示する。メンバーのリストは、アカウントマネージャーを含み、メンバーアカウント名２９４、メンバー名２９６、作成日付２９８、最後にアクセスされた日付３００を表す表で表示される。メンバー名をクリックすると、メンバーに予めアドレス指定されている「メール先：」ボックス（図示せず）が出てくる。アカウント名をクリックすることに依って、マネージャーは、個々のメンバーアカウント情報を見て編集できる。この情報は、グループアカウント情報ページと同様なフォーマットのメンバーアカウント情報ページ（図示せず）に表示される。基本メンバーアカウント情報は、次のものを含む（編集可能な情報はその旨示されている）。

【００６８】・グループアカウント
・メンバーアカウント（編集可能）
・作成日付
・最新アクセス日付

メンバー情報
・メンバー名（編集可能）
・電子メールアドレス（編集可能）

マネージャーは、メンバーのパスワードは見れないが、新しいパスワードを指定し、それを確認することによってメンバーアカウント情報ページにあるパスワードを変更できる。マネージャー或いはメンバー何れかによる最新パスワード変更の日付（図示せず）も表示される。このページにある情報になされたどんな変更も、更新（図示せず）をクリックすることによって提示できる。リセット（図示せず）は、以前に記憶された情報を復元する。

【００６９】メンバーアカウントは、メンバーアカウント情報ページにある削除ボタンをクリックすると完全に削除することができる。アカウントを削除する前に、専用サーバーは、今から行う作業をマネージャーに通知し処理の前に確認を要求する確認ページを出す。メンバーアカウントが更新或いは削除されると、更新された検分メンバーウインドウが表示される。マネージャーは、第二ツールバー１５６にある追加メンバーリンクをクリックすることによりメンバーを追加できる。アカウントマネージャーに、メンバーアカウントの作成に必要とされる情報を促すフォーム（図示せず）が表示される。このフォームは、メンバーが追加されるグループアカウントと、許可された最大総数に対するメンバー数とを示す。必要とされる情報には次のことが含まれる。

【００７０】
・メンバーアカウント名（マネージャーによって作成）
・メンバー名
・メンバーの電子メールアドレス
・パスワード（及び確認パスワード）

追加（図示せず）をクリックすると新しいアカウントが作成され、マネージャーは、更新された検分メンバーウインドウに戻る。リセット（図示せず）をクリックするとフォームをクリアーする。個々のアカウントは、アカウントホルダーを除いてはグループメンバーを有していないので、その様な個々のアカウントホルダーは、メンバー情報ないし機能を有していない。第二ツールバー１５６は、情報（図示せず）とヘルプ（図示せず）しか含んでいない。アカウント情報ページから表示される情報は、現在のメンバー数を除いては、グループアカウント情報ページから利用可能なものと同じである。

【００７１】メンバーアカウントホルダーは、メンバー管理機能も有しておらず、第二ツールバーは、情報（図示せず）とヘルプ（図示せず）のみを含んでいる。メンバーアカウント情報は、マネージャーが見るのと同じ基本情報を含んでいる。しかしながら、メンバーは、電子メールアドレス情報を編集することができるのみである。好適実施例では、メンバーは、メンバーアカウント情報ページにおいて自分自身のパスワードを変更できる。彼らは、現行のパスワードと新しいパスワードを入力し、次に新しいパスワードを確認しなければならない。しかしながら代替実施例では、メンバーは、アカウントマネージャー経由自分のパスワードを変更できるだけである。

【００７２】メインツールバー１５４にあるビリングボタン１４８で、ビリングコードモード管理とインボイス機能にアクセスできる。ビリングボタンをクリックすると、定義されたビリングコードの表３２０が表示される。図１９は、本発明の好適実施例に依るビリングコードウインドウ３０８の画面である。第二ツールバー１５６上のビリング用の第二ナビゲーションは、ビリングコード３１０、追加コード３１２、インボイス作成３１４、インボイス検分３１６、選択３１８、ヘルプ１５８を含んでいる。表は、コードの総数及びどれが現在見られていたものかを示す３２２を表示する。本発明の好適実施例では、ビリングコードは２５文字までの長さで、英字、数字、文字で構成される。

【００７３】各々のビリングコード３２４は、随意選択の簡単な英語記述３２６又はそれに関連する名前を有する。ビリング選択（参照図２４）において、ユーザーは、コード又は記述によってビリングコードを分類するか、及びページ毎に何行表示するかを指定する。選択設定３２８は、表で表示される。ネクスト３３０とプレビアス（図示せず）ボタンに依って、ユーザーは、ビリングコードの追加ページを見ることができる。ビリングコードの二つのレベルがグループアカウントに提供されている。グループマネージャーは、全てのグループメンバーがアクセス可能なコードのリストを保守する。グループメンバーは、頻繁に使用されるコードに容易にアクセスするためにグループリストから自分自身のコードのサブセットを選択できる。

【００７４】メンバーは、ビリングコードを編集及び作成できず、マネージャーが作成したリストからコードを選択して、自分の個人リストに追加しなければならない。メンバーは、ビリング選択にグループ或いは個人ビリングコードを表示するか否かを指定することができる。ホットリンクされたビリングコードをクリックすると、ユーザーは、コード又はその記述を編集又は削除できる。図２０は、本発明の好適実施例に依る編集ビリングコードウインドウ３３２の画面である。ユーザーは、ダイアログにある適切なフィールド３３８、３４０からビリングコード又は記述を編集できる。フィールドの情報はリセットボタン３４２を使ってクリアされる。変更は、更新３３４をクリックしてセーブされ、ユーザーは、更新された情報を表示するビリングコード表に戻る。ユーザーは、このダイアログからコードと記述を削除３３６することもできる。グループメンバーは、グループビリングコードを編集できないので、グループメンバーが見る場合、グループビリングコードはホットリンクされていない。

【００７５】第二ナビゲーションにある追加コード機能３１２は、個人ビリングコードリストに項目を追加するために使用される。図２１は、本発明の好適実施例に依る追加ビリングコードダイアログ３４４の画面である。マネージャーと個々のアカウントホルダーは、新しいコードを「ビリングコード入力：」フィールド３４６に入力する。全ての関連する随意選択記述も、提供されたフォームで「記述：」フィールド３４８に入力される。追加ボタン３５０がクリックされると、ビリングコードリストに新しい情報が追加される。リプレースボタン３５２がクリックされると、ビリングコードリストにある情報が置き換えられる。ビリングコードは、テキストファイルからもアップロード３５４できる。ブラウズボタン３５６は、適切なテキストファイルの位置を突きとめ、アップロードするために使用される。このテキストファイルは、現行のビリングコードリストに置き換えられるか、又はこれに加えられる。新しいコードが首尾よく加えられた場合、ユーザーには、更新されたビリングコードリストが提示される。

【００７６】グループメンバーは、コードをグループビリングコードリストからの自分の個人コードリストに追加できるだけである。グループメンバーが追加コードをクリックすると、グループリストからのコードのリストボックスが提示される。彼らは次にリストボックスから複数のコードを選択できる。一旦希望のコードが選択されると、メンバーは、追加ボタンをクリックして自分の個人リストに選択したコードを追加する。インボイス作成３１４リンクをクリックすると、ユーザーは、インボイスを作成できる。図２２は、本発明の好適実施例に依るインボイス作成ウインドウ３５８の画面である。ダイアログは、ユーザーが、どの送付が現在のインボイスに対する請求なのかを指定することができるサーチスクリーンである。送付は、ビリングコードないし受信者によって請求される。

【００７７】ユーザーは、リスト３６０からビリングコードないしビリングコードのセットを選択するか、或いは受信者の電子メールアドレス３６２を入力する。リストには、ビリングコードとビリング選択に示された関連する記述が含まれている。現在の選択が表示される３６４。ユーザーは、インボイスのビリング期間３６６に関する日付範囲も指定する。一旦適切な情報が入力される

と、ユーザーは作成３６８をクリックして、照会を開始しインボイスを生成する。リセット３７０は、全ての項目をクリアーする。照会結果は、図２３で示す様に、検分インボイスモードにある予めフォーマットされた基本インボイスレポートウインドウ３７２に表示される。ビリングコード３７４とビリング期間３７６は、照会結果を含む表３７８と共に表示される。

【００７８】表は、個々の送付のサブジェクト３８４、送信日付３９０、受信者３９２を表示する。料金３８０と送付の総額３８２も示される。インボイスフォーマットは、ビリング選択に記される。個々の送付のサブジェクト３８４は、上記の様にパッケージ詳細レポートにホットリンクされる。パッケージ詳細にアクセスすると、ナビゲーション状態はビリング／検分インボイスのままである。インボイス検分３１６をクリックすると、表示はインボイスレポートに戻る。エクスポートボタン３８６に依って、ユーザーは、統合のためにタブで区切ったテキストファイルとしてレポートデータを他の現行のビリングシステムにエクスポートできる。インボイスレポート選択３８８（利掛け料金は除く）も表示される。

【００７９】ビリング選択３１８に依って、ユーザーは、ビリングコード管理とインボイスレポートフォーマットに作用する選択を記すことができる。図２４は、本発明の好適実施例に依るビリング選択ダイアログ３９４の画面である。プルダウン３９６に依って、グループメンバーは、個人ビリングコードリスト或いはアカウントマンージャーが保守しているグループビリングコードを使用するかが選べる。全てのユーザーは、ビリングコード３９８ないし記述４００によってリストを表示する様選択する。この選択は、送信オプションとインボイス作成にある選択ボックスでの表示に作用する。選択は、ビリングコード表示表の表示にも作用する。表示がビリングコードでされる場合、第一コラムはビリングコードであり、リストはビリングコードによって分類される。表示が記述で行われる場合、第一コラムは記述であり、リストは記述により分類される。ユーザーは、ページ毎に表示される行の数４０２を指定する。

【００８０】ユーザーは、クライアントに請求する料金４０４を更に記す。この料金は均一料金４０８でもよいし、ユーザーのインターネットサービスプロバイダが請求する費用に加えてパーセンテージ利掛け４０６を含んでいてもよい。ビリング選択ダイアログに表示される情報は、更新４０５或いはリフレッシュされる４０７。インボイスレポートに関して、ユーザーは予め定義されたフォーマット４１０を選択してもよいし、新しいフォーマットを定義４１２してもよい。好適実施例では、ユーザーは、三つの予め定義されたフォーマット、基本インボイス、明細インボイス、ビリングコードインボイスの各フォーマットから選択する。基本インボイスフォーマットは、既に図２３に示した。図２５は、本発明の好適実施例に依る明細インボイスフォーマットでのインボイスレポートの画面である。明細インボイス４１４は、文書サイズ４１８だけでなく個々の送付に関する受信者の総数４１６を表示する。この情報は、入力順に分類される。

【００８１】図２６は、本発明の好適実施例に依るビリングコードインボイスフォーマットでのインボイスレポートである。ビリングコードインボイスフォーマット４２０は、日付同様、ビリングコード４２２によっても分類される。ＣＵＩに依って、発行者と他のユーザーは配布リストを作成及び管理できる。図２７は、本発明の好適実施例に依るメールリストページ４２４の画面である。メールリスト機能は、メインツールバー１５４からアクセス可能である。第二ナビゲーションは、メールリスト４２６、作成リスト４２８、選択５３０、ヘルプ１５８を含む。グループアカウント用に、メールリストに二つのレベルがあり、それはグループと個人である。グループリストは、アカウントマネージャーによって管理されており、全てのグループメンバーがアクセス可能である。グループメンバーは、そのグループメンバーによってのみアクセス可能な個人リストを定義できる。個々のメンバーは、自分のメールリスト選択の中でどのリストのセットを使用するか指定することができる。

【００８２】メインツールバー１５４にあるメールリストボタン１５０をクリックすると、現行メールリスト４３４を表す表４３２を表示する。この表は、個々のメールリストにある受信者の総数４３６とメールリストが最も最近変更された日付４３８を提示する。選択設定４４０も表示される。メールリスト選択（図示せず）において、ユーザーは、項目をメールリスト名で分類するか、日付によって分類するかを指定する。現在の選択が、メールリストダイアログに表示される。ネクストとプレビアスボタン（図示せず）が、メールリストのページ間をナビゲートするために提供されている。メールリストのホットリンクされた名前４４２をクリックすると、選択されたメールリストに関するメールリスト詳細が出てくる。図２８は、本発明の好適実施例に依るメールリスト詳細ウインドウ４４４の画面である。

【００８３】メールリスト詳細ページは現行のメールリストについての一般情報を表示し、ユーザーは、メールリストアドレスを見たり管理したりできる。グループメンバーは、グループメールリストを操作できない。それ故、グループリストのメールリスト詳細は、編集のためのフィールドを表示しない。しかしながらグループメンバーは、個人メールリストを編集できる。アカウントマネージャーは、グループメールリストを操作できる。アカウントマネージャーに提示された詳細４４４は、編集可能なフォームでメールリストの名前４４６を表示する。リストの名前を変えるには、ユーザーは、フォームにある名前を変更し、更新ボタン４４８をクリックす

る。ユーザーは、適切なボタンをクリックして、全体のメールリストを削除４５０、或いはアドレスを追加４５２できる。送受信者４５４と最後に変更された日付４５６も表示される。

【００８４】この詳細はメールリストアドレス４５８も表示する。本発明の好適実施例では、完全なアドレスリストの最初のページは、メールリスト選択で指定されたページ毎の行数に従って表示される。この詳細は、総アドレスからどのアドレスが表示されているかを示す。ネクストとプレビアスリンク（図示せず）は、アドレスの複数ページ間をナビゲートするために提供される。ユーザーは、設けられているフィールド４６０で照会を指定してアドレスの選択セットを見ることもできる。例えば、電子メールアドレス或いはドメイン名の様なアドレスの一部分を指定することもできる。検分ボタン４６２をクリックすると、合致アドレス４５８の表４６４が表示される。表は、アドレスの総合致セットからどのアドレス４６６が表示されているかを示す。

【００８５】ユーザーは、提供されたフィールド４６０に照会を記して、アドレスの選択セットを見ることが更にできる。例えば、電子メールアドレスないしドメイン名の様なアドレスの一部分が記される。検分ボタン４６２をクリックすると、次に合致するアドレス４５８の表４６４が表示される。表は、アドレスの総合致セットの中からどのアドレス４６６が表示されているかを示す。ユーザーは、適切なアドレスをクリックして表にある個々のアドレスを編集ないし削除する。次に、更新と削除ボタンを有する編集ページ（図示せず）が表示される。アドレスが更新ないし削除されると、ユーザーは、更新されたメールリスト詳細ページに戻る。ユーザーは、詳細ページから複数のアドレスを一度に削除することもできる。「ページ上の項目削除」ボタン４６８をクリックすると、表にある全てのアドレスが削除される。「全ての合致項目削除」４７０をクリックすると、アドレスが現在のページで見えるか否かにかかわらず、照会に合致する全ての項目が削除される。専用サーバーが実際にアドレスを削除する前に、ユーザーに作業を確認する様求める警告メッセージが表示される。一旦アドレスが削除されると、詳細ページはすぐに更新されユーザーに示される。

【００８６】メールリスト詳細４４４にある追加アドレスボタン４５２をクリックすると、追加アドレスページが表示される。図２９は、本発明の好適実施例に依る追加アドレスウインドウ４７２の画面である。最新のメールリスト４７４の名前が一番上に表示される。名前は、メールリスト詳細ページにもリンクされる。ユーザーは、追加アドレスを、手動入力４７６により、ファイルからアップロードして、追加できる。ユーザーは、ファイル名４７８を入力することもできるし、全てのファイルをサーチするためにブラウズボタン４８０を使うこともできる。名前は現行のメールリスト４８２から得て、最新メールリストに合体させることもできる。追加アドレスは、最新アドレスリストに追加される４８４か、最新リストに置き替わる４８６。名前が提示された後、ユーザーは、ほんの今起こったばかりの追加ないし置き換えを確認する行が一番上についた、更新されたメンバー詳細ページに戻る。

【００８７】ユーザーは、第二ナビゲーションから作成リストリンク４２８をクリックすることにより新しいメールリストを作成できる。本発明の好適実施例では、作成メールリストページ（図示せず）は、追加アドレスページと同じである。しかしながら、作成メールリストページでは、ユーザーはメールリストの名前を督促される。ユーザーはアドレスを、設けられたテキストボックスで手動で入力できる。代りに、ユーザーは、ファイルからアドレスをアップロードするか、又は現行メールリストからアドレスをコピーすることもできる。しかしながら、ユーザーが新しいリストを作成するので、現行リストに置き替えるためのオプションはない。追加をクリックすると、指定された名前とアドレスのあるメールリストが作成される。ユーザーに、新しいリスト情報を含んだ、更新されたメールリストレポートが提示される。

【００８８】本発明は、システムへのアクセスを認められたユーザーに制限する機密保護を更に提供する。本発明によってサポートされる機密保護のタイプは、認証レイヤー、セキュアソケットレイヤー、パスワード保護、プライベートキー暗号化、パブリックキー暗号化、証明認証を含む。この機密保護は、送信クライアントアプリケーション、受信クライアントアプリケーション、ＣＵＩの内の少なくとも一つにおける少なくとも一つの機密保護モジュールを含む機密保護フレームワークによって提供される。図３０は、本発明に依る電子ネットワーク上での文書送付に関する方法のフローチャートである。送信コンピューターは、例えば、インターネット上でセッション（５００）を確立する。送信コンピューターは、次に送信クライアントアプリケーションを使ってこの電子ネットワーク上で専用サーバー（５０５）に文書を送付する。

【００８９】送信クライアントアプリケーションは、文書送信、文書作業リスト表示、文書追跡、文書パラメーター指定と記憶、機密保護特徴提供用のモジュールを含むのが好ましい（５１０）。これらモジュールの幾つか或いは全ては、特定のセッションの間アクセスできる。専用サーバーは文書を記憶し（５１５）、電子通知メッセージを受信装置に送る（５３０）。専用サーバーはコンフィギュレーションユーザーインターフェース経由で管理される（５２０）。コンフィギュレーションユーザーインターフェースは機密保護特徴モジュールと同様に、文書送信、文書追跡、アカウンティング、ビリング、メールリスト生成用のモジュールを含んでいるのが

好ましい（５２５）。

【００９０】通知メッセージに応じて、受信装置は受信クライアントアプリケーションを使って専用サーバーから文書をダウンロードする（５３５）。受信クライアントアプリケーションは、機密保護提供用と同様に文書をダウンロード、検分、操作するためのモジュールを含んでいるのが好ましい（５４０）。本発明は、本文において好適実施例に関して述べられているが、当業者には、他の応用例が本発明の精神と範囲から逸脱することなく本文に述べられているものと取って替われることは既に明らかであろう。本発明は、よく知られているプログラミング技術と装置を使って当業者により容易に組み立てられ構成される。例えば、本文に述べられるデスクトップ表示にあるツールバーとメニューの配置と内容は、説明のためのものである。更に、本発明の機能は、アイコンやキーボードテキスト入力を含む代替方法によってアクセスされてもよい。

【００９１】本発明の一実施例において、文書送付に関する通知メッセージは、通知受信装置で受信される。すると、文書は、通知受信装置に含まれているか或いはそこから独立している受信装置で検索される。例えば、通知メッセージは、ページャー又はパーソナルデジタルアシスタントで受信でき、文書は、ウエブブラウザを使ってパーソナルコンピューターで受信できる。送信者がデジタル証明登録の実行を一人或いはそれ以上の受信者クライアントに対し開始及び制御できるようにすることにより、会社、発行者、個人が、送信者操作証明登録システム（ＳＤＣＥ）４２によって、電子的に文書を安全に配布できるようになる。図３１は、インターネットを含むネットワーク１３４４を通して、送信コンピューター１３５２と受信コンピューター１３７０間で実行される基本証明登録システム１３４２ａを示す。図３２は、送信コンピューター１３５２、ＳＤＣＥサーバー１３５８、受信コンピューター１３７０間で実行される証明登録システム１３４２ｂを示す。図３３は、送信コンピューター１３５２、ＳＤＣＥサーバー１３５８、データベースサーバー１３６２、受信コンピューター１３７０間で実行される証明登録システム１３４２ｃを示す。図３４は、送信コンピューター１３５２、ＳＤＣＥサーバー１３５８、データベースサーバー１３６２、証明サーバー１３８８、受信コンピューター１３７０間で実行される証明登録システム１３４２ｄを示す。

【００９２】送信者操作証明登録システム１３４２によって、文書１３１２の送信者１３５２は、文書の対象受信者１３７０のためにデジタル証明１３４５の生成（図３５参照）を開始できる。文書１３１２は、特定コンピューターファイル又はより一般的なあらゆる個別データの集まりを意味する。送信者操作証明登録システム１３４２は、文書の対象受信者１３７０のためのデジタル証明生成に関連する複雑さを単純にし、証明生成の基本的な負担を（現在多くのシステムがサポートしている）受信者１３７０から送信者１３５２へ移す。図３５は、デジタル証明１３４５を示しており、パブリックキー１３３２とプライベートキー１３４０から成るキーペアー示しており、パブリックキー１３３２は、対象受信者１３７０の様な特定のエンティティに関連付けられ、発行される。

【００９３】安全な文書送付に関連する主要問題の一つは、対象受信者１３７０のパブリックキー１３３２を使って文書を暗号化１３１２する試みから生ずる。特に、文書の対象受信者１３７０がデジタル証明１３４５を持っていない場合である。送信者１３５２がアクセス可能な受信者１３７０のデジタル証明１３４５が無い場合は、文書１３１２の送信者１３５２は、受信者のパブリックキー１３３２を使って文書１３１２を暗号化できず、その結果、文書１３１２が招かざるアクセスから保護されることを保証できない。送信者操作証明登録システム１３４２に依って、文書１３１２の送信者１３５２は、対象受信者１３７０のためにデジタル証明１３４５を活動的に生成する処理を開始し、それによって対象受信者１３７０に課す要求は最小限になる。

【００９４】送信者操作証明登録システム１３４２は、証明生成の負担を所定の文書１３１２の受信者１３７０から送信者１３５２に移す。送信者操作証明登録システム１３４２は、文書送付に関連して、文書１３１２の送信者１３５２が多くの場合対象受信者に関する独特且つ特定の情報を持っている事実を利用する。例えば、弁護士がクライアント１３７０に文書を送信すると仮定する。弁護士１３５２は、クライアントの電子メールアドレス、実際のアドレス、電話番号の様な特定情報を含むクライアント１３７０に関連する記録を所有しているはずである。クライアント記録は、クライアントの社会保障番号、運転免許証番号、更にはクレジット情報の様な極秘情報も含んでいるかもしれない。一般的に所定の個人或いはエンティティ１３７０を認証するために利用されるのは、このタイプの極秘情報であり、その結果デジタル証明１３４５が生成されるのである。極秘性の高く特別な情報は、高レベルの認証を生み出し、その結果が、安全なデジタル証明である。

【００９５】それ故、送信者操作登録システム１３４２は、送信者１３５２が文書１３１２の対象受信者１３７０に関する重要な極秘情報を多くの場合知っているという事実を利用する。デジタル証明１３４５を生成するために送信者１３５２がこの極秘情報を使用することによって、受信者１３７０にその身元を確認するために課される負担は最小になる。送信者１３５２は、デジタル証明１３４５を使って、文書１３１２を対象受信者１３７０に安全に送信する。システム実行。上記例において、送信者である弁護士１３５２は、対象受信者であるクライアント１３７０に極秘文書を送信したい。弁護士１３

５２がアクセス可能なデジタル証明１３４５を現在持っていないクライアント１３７０に対して、弁護士１３５２は、クライアント１３７０用のデジタル証明１３４５を生成するため、送信者操作登録システム１３４２を呼び出すことができる。

【００９６】最初に、送信者操作登録システム１３４２は、デジタル証明１３４５が受信者であるクライアント１３７０用にあるかどうかを決めるために、データベース１３４６をチェックないし照会する。無い場合、送信者操作登録システム１３４２は、一般的にはクライアントの特定且つ極秘情報を含むクライアント１３７０に関する記録を引き出すためにデータベース照会を行う。送信者操作登録システム１３４２は次に、図３６に示す様に、証明要覧１３４７を生成する。この証明要覧１３４７は、クライアント特定データ１３４８、生成する証明の型１３４９（例えばX．５０９証明）を含むクライアント１３７０に関するデジタル証明生成に必要な情報の殆どを含んでいる。好適実施例では、証明要覧１３４７は、安全なＳＤＣＥサーバー１３５８に送られる。ＳＤＣＥサーバー１３５８は次に、極秘情報１３４８の独立確認を求めてクライアント１３７０に「コンタクト」する。例えば、本発明の好適実施例では、ＳＤＣＥサーバー１３５８は、独自の動的生成されたＵＲＬ（ユニフォームリソースロケータ）を使ってクライアント１３７０に電子メールメッセージを送る。すると、クライアント１３７０は、標準ウエブブラウザを通してこのＵＲＬに「クリック」或いはアクセスできる。ＵＲＬにアクセスすると、クライアント１３７０とＳＤＣＥサーバー１３５８間で直接対話或いはＳＤＣＥ会話１３６８が始まる。

【００９７】クライアント１３７０は一般的に、一つ或いはそれ以上の極秘情報１３４８をＳＤＣＥサーバー１３５８に入力する様求められる。好適実施例では、会話は、クライアント１３７０とＳＤＣＥサーバー１３５８の間のセキュアソケットレイヤー（ＳＳＬ）上で行われ、ＨＴＭＬフォームを利用する。ＳＤＣＥサーバー１３５８は次に、入力された情報を記憶された証明要覧１３４７内にある記憶されたクライアント情報と比較して、クライアント１３７０が正しいかどうか立証する。合致すると、ＳＤＣＥサーバー１３５８は、安全なチャンネル上で受信者クライアントデスクトップ１３７２に証明要覧１３４７を送り、受信者システム上でキーペアー１３３２、１３４０を生成するために証明要覧１３４７を使用するソフトウエアを受信クライアント１３７０に配布する。本発明の好適実施例では、このソフトウエアは、簡単なジャバアプレットであり、ブラウザを通して受信者１３７０に包み隠さず送られる。生成されたプライベートキー１３３２は、好ましくはＰＫＣＳ１２フォーマットを使って、受信者システム１３７０に記憶される。パブリックキー１３３２はＳＤＣＥサーバー１３５８に戻されるが、このＳＤＣＥサーバー１３５８は普通、パブリック及びクライアント情報の両方をデジタル証明１３４５として、ＬＤＡＰないし（カナダ、オタワのエントラスト株式会社の）エントラスト証明管理サーバーの様な証明サーバー１３８８上で記録している。

【００９８】これで、送信者（例えば弁護士）１３５２は、対象受信者クライアント１３７０用の記憶されたパブリックキー１３３２にアクセスし、パブリックキー１３３２を使って受信者クライアント１３７０を対象とした文書１３１２を暗号化し、そして、暗号化された文書１３３６をクライアント１３７０に送信することができる。次に、クライアント１３７０が、個人受信者システム１３７０に現在ある（パブリックキーと）対応するプライベートキー１３４０を使って暗号化された文書１３３６を解読する１３３８。図３７は、送信者操作証明登録システム１３４２の第一段階を示す。送信者１３５２はステップ１３５６で、ＳＤＣＥサーバー１３５８にコンタクトし、受信者を確認するために電子メールアドレスの様な基本情報を送って、受信者１３７０に関する証明の生成を開始する。

【００９９】ＳＤＣＥサーバー１３５８は次にステップ１３６０で、社会保障或いは個人アドレスの様な対象受信者１３７０に特定の極秘情報１３４８に関するデータベース１３４６を照会する。データベース１３４６は、独立データベースサーバー１３６２内或いはＳＤＣＥサーバー１３５８内の様ないろいろな場所のどこにあってもよい。使用可能極秘情報１３４８が対象受信者１３７０のためににある場合、ステップ１３６４で、データ記録としてＳＤＣＥサーバー１３５８に送られる。ＳＤＣＥサーバー１３５８は次にステップ１３６５で、データ記録を使って証明要覧１３４７を生成するが、これは後で、受信者１３７０を立証し、デジタル証明１３４５を生成するために使用されることになる。

【０１００】図３８は送信者操作証明登録システム１３４２の第二段階１３６６を示すが、これは立証会話と呼ばれる。ＳＤＣＥサーバー１３５８は証明要覧１３４７を取り、ステップ１３６８で、文書１３１２の対象受信者１３７０と直接対話を開始する。この直接対話１３６８は、対象受信者１３７０にクライアント特定データ１３４８を要請する。本発明の好適実施例では、ＳＤＣＥサーバー１３５８は、動的に生成されたユニフォームリソースロケータ（ＵＲＬ）を使って電子メールメッセージを送信する。生成されたＵＲＬをクリックして、受信者１３７０は、ＳＤＣＥサーバー１３５８との直接対話１３６８を呼び出す。この時点で、ＳＤＣＥサーバー１３５８は、受信者１３７０からの特定情報を要請するＨＴＭＬフォームを提示する。

【０１０１】ＨＴＭＬフォームと要求される個人情報１３４８は、受信者１３７０に送信される文書１３１２に要望される機密保護のレベルによって変わってもよい。

例えば、高い機密保護レベルを必要としない文書の場合、フォームは確認ボタンを要求するだけでもよい。高い機密保護レベルを必要とする文書の場合、フォームは対象受信者１３７０に、個人アドレス、社会保障番号、被雇用者番号、個人身分証明番号（ＰＩＮ）の様な特定個人情報１３４８の提示を求めてもよい。本発明の好適実施例では、ＳＤＣＥサーバー１３５８と受信者１３７０の間のこの対話は、ＳＳＬを使って安全なチャンネル上で行われる。送られた個人情報１３４８を使って、ステップ１３７４の間、ＳＤＣＥサーバーは、送られたデータ１３４８を対象受信者１３７０に関する証明要覧１３４７と比較して受信者１３７０を立証する。送られた情報１３７４と証明要覧１３４７に適切に記憶された情報１３４８が合致する場合、受信者１３７０はステップ１３７５で認証され、処理は次の段階に続く。送られた情報１３７４と証明要覧１３４７に適切に記憶された情報１３４８が合致しない場合、送信者１３５２には、デジタル証明１３４５が生成されていないと通知される（図４１）。

【０１０２】図３９は、送信者操作証明登録システム１３４２の第三段階１３７６を示し、これはパブリック／プライベートキーペアー生成と呼ばれる。立証会話段階１３６６上で要請された個人情報１３７４が、ＳＤＣＥサーバー１３５８で証明要覧１３４７に合致したと仮定すると、ＳＤＣＥサーバー１３５８は次にステップ１３７８で、ソフトウエアと証明要覧１３４７を受信者システム１３７０に送る。送られたソフトウエアは、証明要覧１３４７と受信者コンピューター１３７０に特有の情報を利用し、プライベート／パブリックキーペアー１３３２、１３４０から成るデジタル証明１３４５を生成する。キーペアー１３３２、１３４０は、送信され、送信者システム１３５２で局地的に記憶される。好適実施例では、パブリック／プライベートキーペアー１３３２、１３４０は、ＰＫＣＳ１２フォーマットに記憶される。次に、パブリックキー１３３２と受信者１３７０に関する証明要覧１３４７のリファランスは、受信者１３７０からＳＤＣＥサーバー１３５８に送られる。

【０１０３】図４０は、送信者操作証明登録システム１３４２の第四段階１３４８を示し、これは受信者パブリックキー１３３２の送信と登録と呼ばれる。処理のこの段階で、対象受信者１３７０に関するパブリックキー１３３２は、受信者システム１３７０からＳＤＣＥサーバー１３５８に送られる。ＳＤＣＥサーバー１３５８はステップ１３８６で、デジタル証明１３４５として結合されたパブリックキー１３３２と証明要覧１３４７を証明サーバー１３８８に送る。好適実施例では、証明サーバー１３８８は、ＬＤＡＰ（ライトウエイトディレクトリアクセスプロトコル）サーバーである。次に、ＳＤＣＥサーバー１３５８は、図３で示す様に文書１３１２が受信者１３７０のパブリックキー１３３２を使って現在暗号化１３３４できることを示す通知を、ステップ１３９０で送信者１３５２に送信する。次に、暗号化された文書１３３６は、一般的にはネットワーク又はインターネットアーキテクチャ１３４４を通して受信者１３７０に送付される。受信者１３７０は次に、図４に示す様に、情報を解読するために自分自身のプライベートキー１３４０を使う。

【０１０４】実行。このセクションは、送信者操作証明登録システム１３４２を構成するための構成要素の全体像を提供する。証明サーバー１３８８の様な構成要素の幾つかは、カスタマゼーション或いは展開を必要としない。図４１は、システムに関するコントロールの流れを説明する基本フローチャートである。送信者デスクトップクライアントソフトウエア。送信者コンピューター１３５２のデスクトップ１３５４上では、送信者操作証明登録システム１３４２は、受信者１３７０と関連するパブリックキー１３３２を照会するためにＳＤＣＥサーバー１３５８及び証明サーバー１３８８に通信するソフトウエアを含んでいる。受信者ソフトウエア構成要素は、受信者１３７０に関するパブリックキー１３３２の検索時に、通常パブリックキー１３３２を使って文書１３１２を暗号化し、次に受信者１３７０へ続いて送付するために文書をＳＤＣＥサーバー１３５８に送る。

【０１０５】ＳＤＣＥサーバーソフトウエア。ＳＤＣＥサーバーソフトウエアは、本発明の好適実施例では、全てのＨＴＴＰ要求を遮断し、転送するためのカスタマイズされたフィルターを有するＨＴＴＰウエブサーバーと、通知を対象受信者１３７０に送る電子メールサーバーと、データベースサーバーを照会し、証明要覧１３４７を生成し（上記記載）、システムの全ての他の構成要素と対話するための基本ソフトウエアとロジックとを含んでいる。ウエブサーバーは、ＳＤＣＥサーバー１３５８と文書１３１２の対象受信者１３７０間の主たるインターフェースであり、そこでＳＤＣＥサーバー１３５８はデジタル証明１３４５の構築を援助する。本発明の好適実施例では、ＳＤＣＥサーバーソフトウエアは、動的に個人ＵＲＬを生成して、対象受信者１３７０と立証会話１３６６（図３８）を開始する。個人ＵＲＬは、受信者１３７０を独自に確認するキーを含み、次にこの「キー」を標準電子メール通知上で受信者に送る。受信者１３７０が（実際は個人ＵＲＬである）この「キー」にアクセスすると、ＳＤＣＥサーバー１３５８はキーを所定の証明要覧１３４７と関連付け、次にウエブインターフェースを通して、立証会話１３６６を行い、所与の受信者１３７０が証明要覧１３４７のパラメーターに合致することを証明する。

【０１０６】受信者クライアントソフトウエア。送信者操作証明登録システム１３４２は、証明要覧１３４７からパブリック／プライベートキーペアーを作成し、これは、ＳＤＣＥサーバー１３５８から受信者システム１３

７０に送られる。受信者コンピューターにあるクライアントソフトウエアは、証明要覧１３４７を取り、受信者デスクトップ１３７２でパブリック／プライベートキーペアー１３３２、１３４０を構成し、受信者システム１３７０でこれらのキー１３３２、１３４０を記憶し、次にパブリックキー１３３２をＳＤＣＥサーバー１３５８に送る。ある好適実施例では、受信者クライアントソフトウエアは、ジャバアプレットであり、ウエブブラウザ経由で包み隠さず且つ動的にダウンロードされ、これを使って、受信者は上記の様にＵＲＬに簡単にアクセスする。

【０１０７】証明サーバー。本発明は、基本デジタル証明管理を利用している。証明サーバー１３８８は、デジタル証明が受信者所定特定ユーザープロファイル（例えば電子メールアドレス及び識別名）があるかどうか決定する照会能力を含む。証明サーバー１３８８は、更新能力も含んでおり、プログラム上のインターフェースが新しい証明をサーバーのデータベースに追加できるようになっている。好適実施例では、ＬＤＡＰ、Ｘ．５００、或いはエントラストサーバーの様な占有の証明サーバーは証明サーバー１３８８として使用できる。データベースサーバー。本発明の好適実施例では、ＳＤＣＥサーバー１３５８は、証明要覧１３４７を構成するために受信者情報を含むデータベース１３４６を照会する。基本実施例では、送信者のデスクトップ１３５４は、内部データベース１３４６を照会でき、又、送信者のデスクトップ１３５４は、デスクトップ１３５４から直接情報を簡単にロードできる。ＳＤＣＥサーバー１３５８によって提供される好適データベース照会は、更なる規模と拡張性をサポートする。

【０１０８】本発明の基本設計に加えて、デスクトップ１３５４から直接に、又はデータベース照会経由での何れかで送信者システム１３５２から容易にアクセス可能な受信者データ１３４８が無い場合の状況が残っている。この場合、送信者操作登録システム１３４２はなお価値を持ち続ける。証明要覧１３４７は制限された情報１３４８を含んでいるが、立証のレベルも又制限されている。しかしながら、基本立証はなお行え、システム１３４２は、受信者１３７０のために基本デジタル証明１３４５を生成する処理をなお簡素化する。この場合、システムは、より単純化された会話１３６６と証明要覧１３４７であることを除いて、設計された様に正確に作動する。図４１は、送信者操作登録システム１３４２の後ろにある基本決定ツリーを説明するフローチャート１３０２である。

【０１０９】ステップ１０２で、送信者１３５２は、文書１３１２に関する対象受信者１３７０のパブリックキー１３３２を証明サーバー１３８８に照会する。パブリックキー１３３２がある場合、文書１３１２は、パブリックキー１３３２を使って暗号化され、ステップ１０４で受信者１３７０に送信される。パブリックキー１３３２が存在しない場合、送信者は、ステップ１３５６で対象受信者１３７０に関する証明要覧１３４７をＳＤＣＥサーバー１３５８に照会する。ＳＤＣＥサーバー１３５８は次にステップ１３６０で、対象受信者１３７０に関する情報１３４８をデータベース１３４６に照会する。情報が在り、データベース１３４６に既に記憶されている場合、ＳＤＣＥサーバー１３５８は、ステップ１３６５でクライアント１３７０に関する豊富な証明要覧を生成する。情報１３４８が無く、データベース１３４６に記憶されていない場合、ＳＤＣＥサーバー１３５８は、ステップ１３６４で簡素化された承認要覧１３４７を生成する。

【０１１０】ステップ１３６８で、ＳＤＣＥサーバー１３５８は、受信者１３７０と立証会話１３６６を開始する。情報１３４８に合致しない場合、ＳＤＣＥサーバー１３５８は、ステップ１０６で送信者に通知し、キーペアー１３３２、１３４０の生成は行われない。合致していれば、ステップ１３８０で、受信者１３７０に関するプライベート／パブリックキーペアー１３３２、１３４０が受信者システム１３７０において生成される。次にステップ１３８２で、キーペアーはＳＤＣＥサーバー１３５８に送られる。ステップ１３８８で、ＳＤＣＥサーバーは、証明サーバー１３８８を使って対象受信者１３７０に関する証明を登録する。ステップ１３９０で、ＳＤＣＥサーバーは、送信者１３５２にデジタル証明１３４５を通知する。すると、送信者１３５２は、図３に示す様に対象受信者１３７０の生成されたパブリックキー１３３２を使って文書１３１２を暗号化できる。暗号化された文書１３３６が、一般的にはネットワーク１３４４上で受信者１３７０に送信されると、受信者１３７０は、図４に示す様に記憶されたプライベートキー１３４０を使って暗号化された文書１３３６を解読できる。

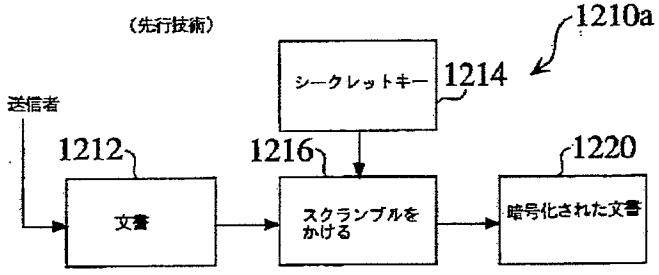
【０１１１】送信者操作証明登録システムとその使用方法がインターネットでの使用と結びつけて本文で説明してあるが、本発明は、希望されるインターネット、イントラネット、ＬＡＮｓとＷＡＮｓ、ないしそれらの全ての組み合わせを含む幅広い種類のネットワークの何れにも適用できる。その上、本発明は、希望される、広範な種類のコンピュータープラットフォーム、サーバー、通信プロトコル、暗号作成プロトコル、或いはそれらの全ての組み合わせにも適用できる。本発明は、特定の好適実施例に関して詳細に説明してきたが、本発明が関係する当業者には、請求項の精神と範囲から逸脱することなく様々な変更修正と改良がなされることは明白である。従って、本発明は請求項によってのみ制限されるものである。

【図面の簡単な説明】

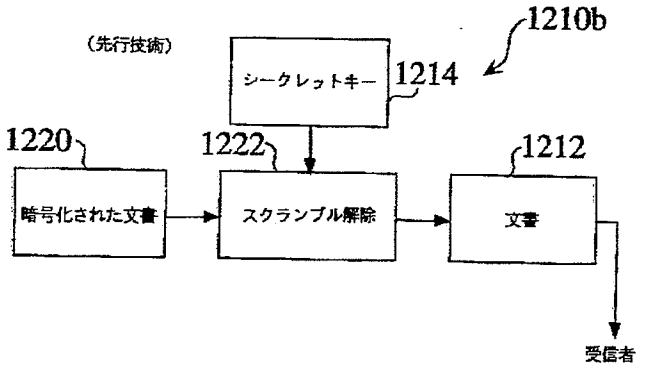
【図１】文書のシークレットキー暗号化のブロック線図である。

【図２】文書のシークレットキー解読のブロック線図である。
【図３】文書のパブリックキー暗号化のブロック線図である。
【図４】文書のプライベートキー解読のブロック線図である。
【図５】本発明に依る文書送付システムの線図である。
【図６】本発明に依るアプリケーションウインドウの画面である。
【図７】本発明に依る文書作業を示すアプリケーションウインドウの画面である。
【図８】本発明の好適実施例に依るパッケージウインドウの画面である。
【図９】本発明に依る受信者のウインドウの画面である。
【図１０】本発明に依るＣＵＩアプリケーションウインドウの画面である。
【図１１】本発明に依るＣＵＩパッケージウインドウの画面である。
【図１２】本発明に依るＣＵＩオプションページの画面である。
【図１３】本発明に依るＣＵＩ追跡サーチページの画面である。
【図１４】本発明に依るＣＵＩ追跡レポート選択ダイアログの画面である。
【図１５】本発明に依る、基本フォーマットにおける受信者要約追跡レポートの画面である。
【図１６】本発明に依る、基本フォーマットにおける受信者詳細追跡レポートの画面である。
【図１７】本発明に依る、ビリングコードフォーマットにおける受信者詳細追跡レポートの画面である。
【図１８】本発明に依る、グループアカウントマネージャーアカウントー検分メンバーウインドウの画面である。
【図１９】本発明に依るビリングコードウインドウの画面である。
【図２０】本発明に依る編集ビリングコードダイアログの画面である。
【図２１】本発明に依る追加ビリングコードダイアログの画面である。
【図２２】本発明に依るインボイス作成ページの画面である。
【図２３】本発明に依る基本インボイスレポートウインドウの画面である。
【図２４】本発明に依るビリング選択ダイアログの画面である。
【図２５】本発明に依る、特定インボイスフォーマットにおけるインボイスレポートの画面である。
【図２６】本発明に依る、ビリングコードインボイスフォーマットにおけるインボイスレポートの画面である。
【図２７】本発明に依るメールリストページの画面である。
【図２８】本発明に依るメールリスト詳細ページの画面である。
【図２９】本発明に依る追加アドレスページの画面である。
【図３０】本発明に依る、電子ネットワーク上での文書送付に関する方法のフローチャートである。
【図３１】ネットワーク上での送信コンピューターと受信コンピューター間で実行される基本証明登録システムを示す。
【図３２】送信コンピューター、ＳＤＣＥサーバーと受信コンピューター間で実行される証明登録システムを示す。
【図３３】送信コンピューター、ＳＤＣＥサーバー、データベースサーバーと受信コンピューター間で実行される証明登録システムを示す。
【図３４】送信コンピューター、ＳＤＣＥサーバー、データベースサーバー、証明サーバーと受信コンピューター間で実行される証明登録システムを示す。
【図３５】デジタル証明のブロック線図である。
【図３６】証明要覧のブロック線図である。
【図３７】送信者操作の証明登録システムにおける操作の第一段階を示す。
【図３８】送信者操作の証明登録システムの第二の立証対話段階を示す。
【図３９】送信者操作の証明登録システムの第三のパブリック／プライベートキーペアー生成段階を示す。
【図４０】送信者操作の証明登録システムの第四段階を示し、受信者パブリックキーの送信と登録と呼ばれる。
【図４１】送信者操作の証明登録システムにおける基本決定ツリーを示すフローチャートである。

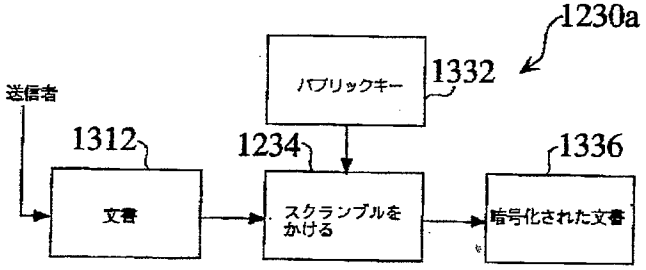
【図１】



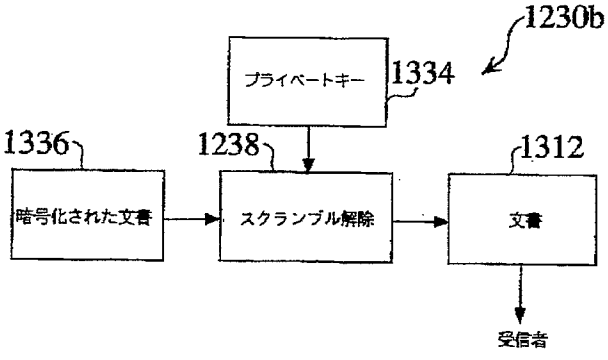
【図２】



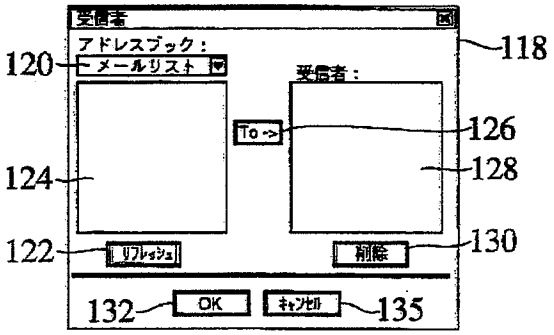
【図３】



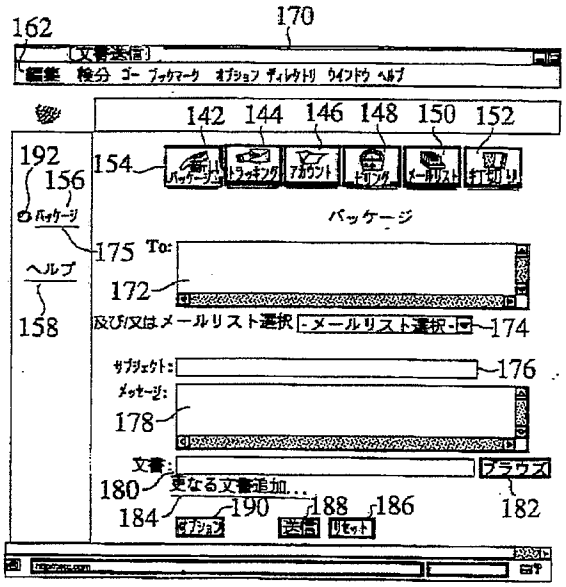
【図４】



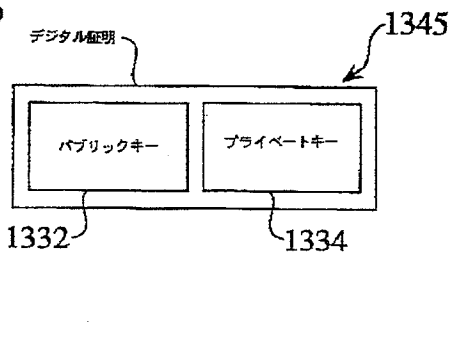
【図９】



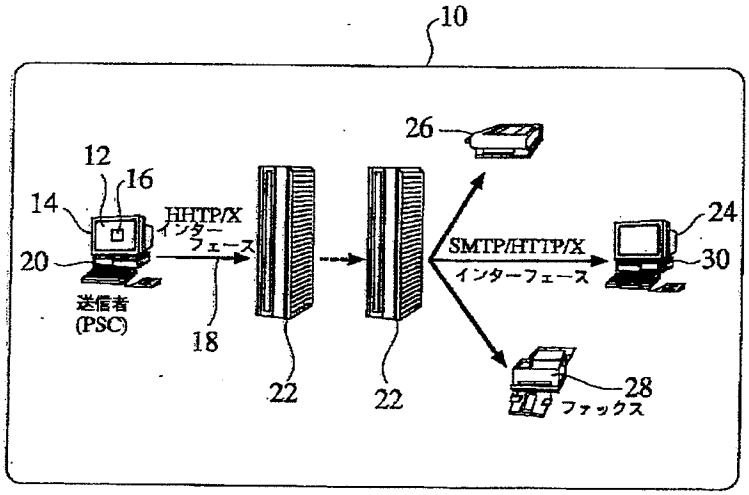
【図１１】



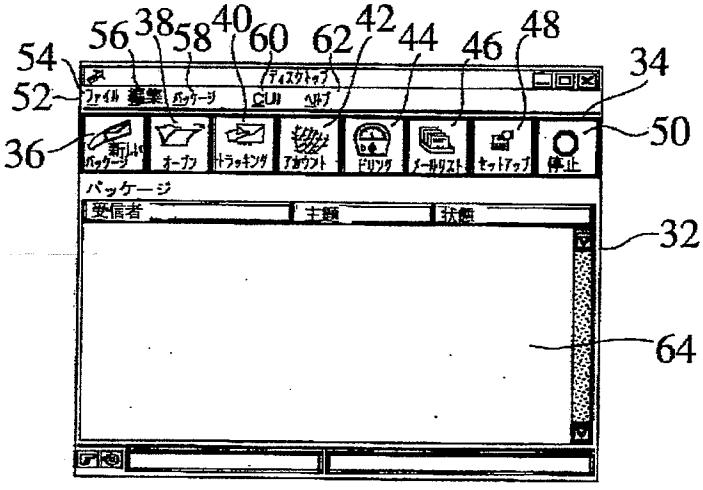
【図３５】



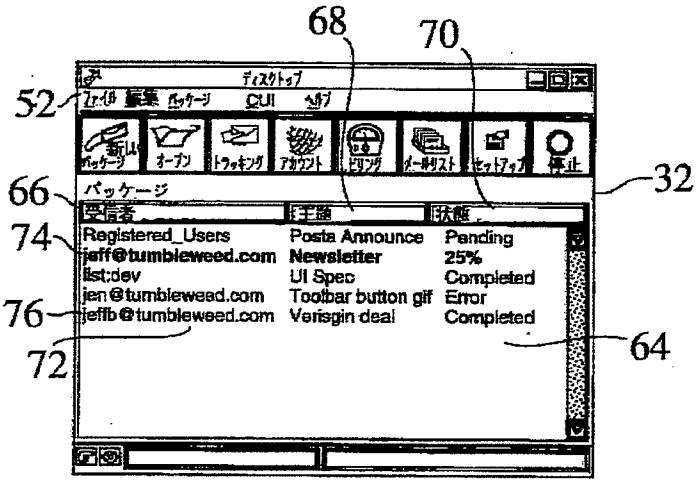
【図５】


10
26
12
16
14
HHTP/X
インター
フェース
20
送信者
(PSC)
18
22
22
SMTP/HTTP/X
インターフェース
24
30
28
ファックス

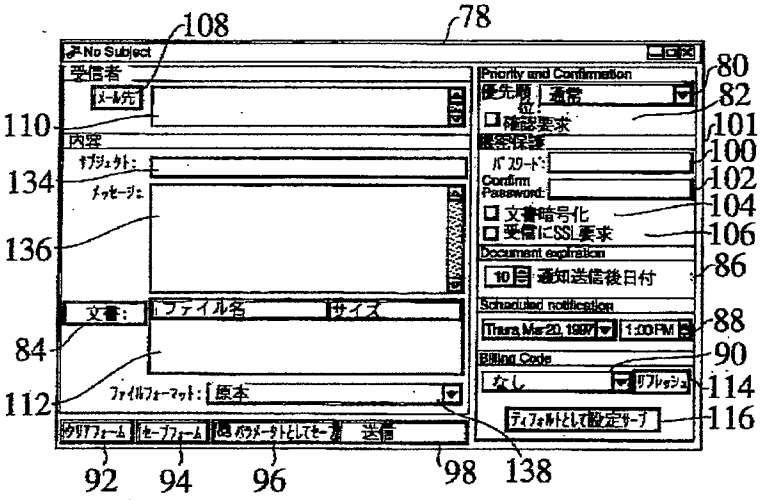
【図６】


56
38
58
40
60
62
42
44
46
48
54
52
34
36
50
ファイル
編集
パッケージ
CUI
ヘルプ
ディスクトップ
新しい
パッケージ
オープン
トラッキング
アカウント
ドリング
メーリングリスト
セットアップ
停止
パッケージ
受信者
主題
状態
32
64

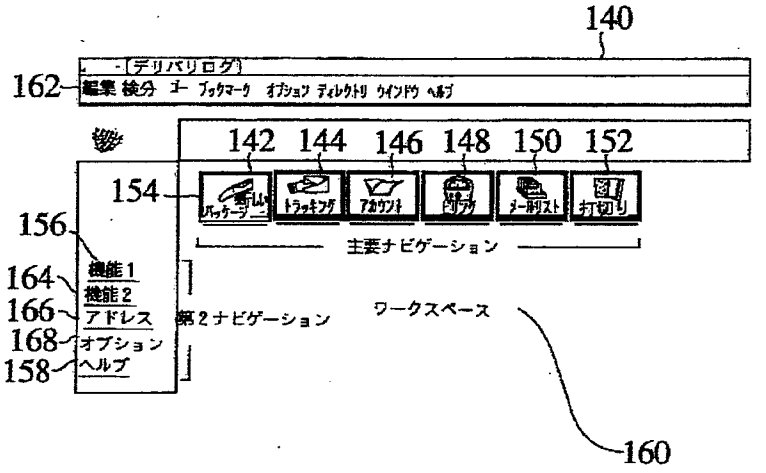
【図７】


68
70
52
ディスクトップ
ファイル 編集 パッケージ GUI ヘルプ
新しい パッケージ
オープン
トラッキング
アカウント
ビリング
メーリングリスト
セットアップ
停止
32
パッケージ
66
受信者
主題
状態
74
Registered_Users
Posta Announce
Pending
jeff@tumbleweed.com
Newsletter
25%
list:dev
UI Spec
Completed
jen@tumbleweed.com
Toolbar button gif
Error
76
jeffb@tumbleweed.com
Verisgin deal
Completed
72
64

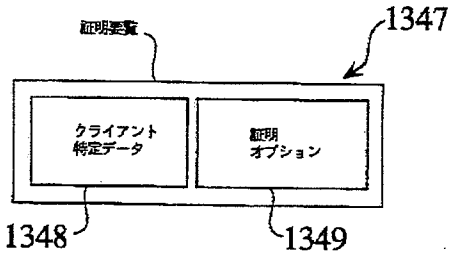
【図８】


108
78
No Subject
受信者
メール先
110
内容
サブジェクト:
134
メッセージ:
136
文書:
ファイル名
サイズ
84
112
ファイルフォーマット:
原本
セーブフォーム
パラメータとしてセーブ
送信
92
94
96
98
138
Priority and Confirmation
80
優先順位:
通常
82
確認要求
101
機密保護
パスワード:
100
Confirm Password:
102
文書暗号化
104
受信にSSL要求
106
Document expiration
10日 通知送信後日付
86
Scheduled notification
Thurs, Mar 20, 1997
1:00 PM
88
Billing Code
90
なし
リフレッシュ
114
ディフォルトとして設定サーブ
116

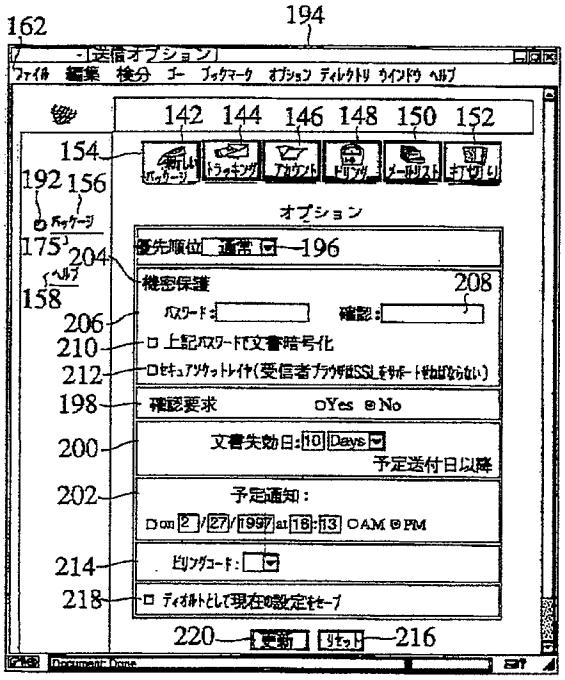
【図１０】



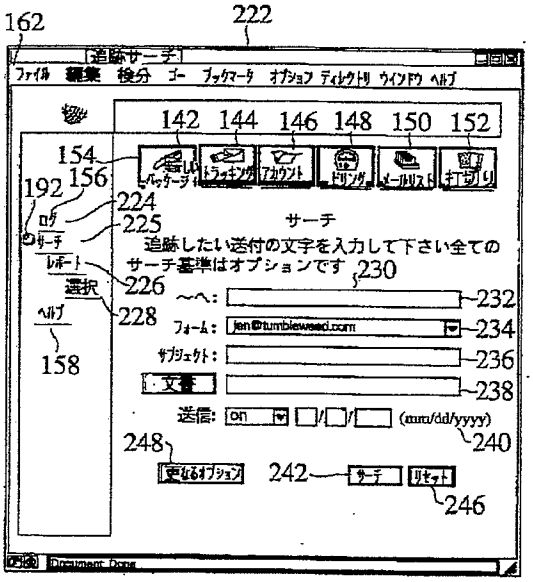
【図３６】



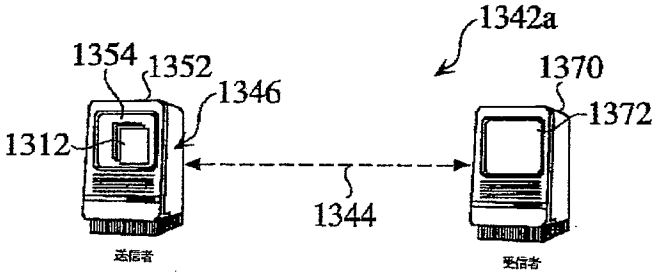
【図１２】



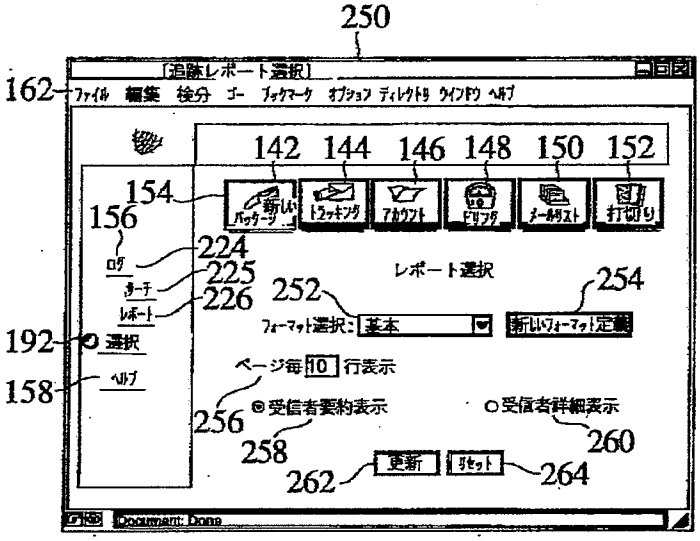
【図１３】



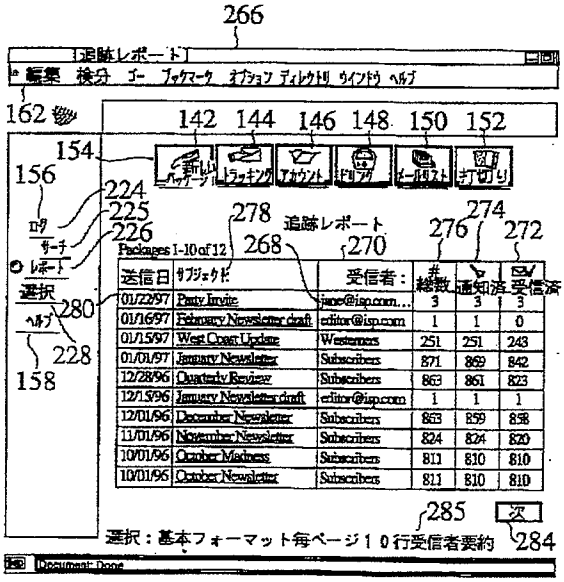
【図３１】



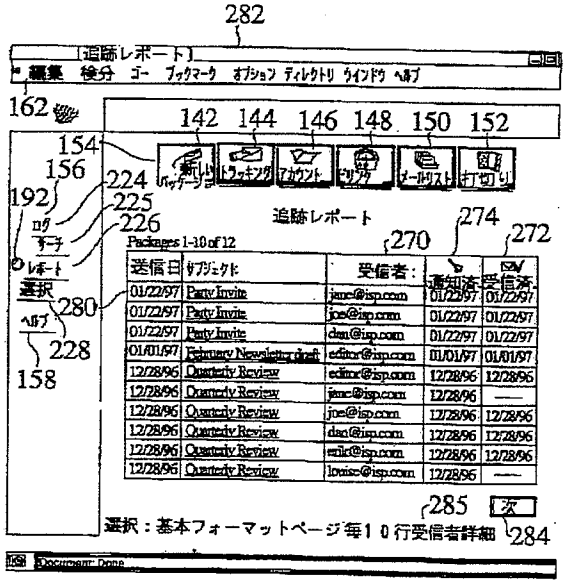
【図１４】


250
追跡レポート選択
162
ファイル 編集 検分 ゴー ブックマーク オプション ディレクトリ ウインドウ ヘルプ
142 144 146 148 150 152
154
156
ログ
サーチ
レポート
224
225
226
192
選択
ヘルプ
158
252
レポート選択
フォーマット選択：基本
254
新しいフォーマット定義
ページ毎 10 行表示
256
受信者要約表示
258
受信者詳細表示
260
262
更新
リセット
264
Document: Done

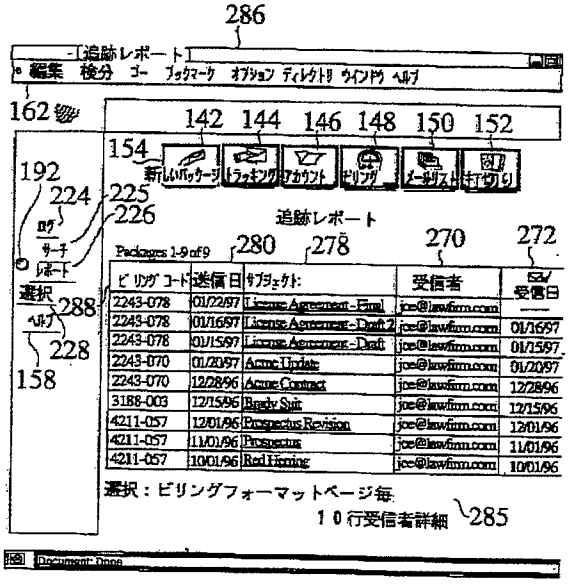
【図１５】


266
追跡レポート
162
142 144 146 148 150 152
154
156
224
225
226
278
追跡レポート
268
270
276
274
272
Packages 1-10 of 12
送信日
サブジェクト
受信者：
総数
通知済
受信済
01/22/97 Party Invite jane@isp.com... 3 3 3
01/16/97 February Newsletter draft editor@isp.com 1 1 0
01/15/97 West Coast Update Westerners 251 251 243
01/01/97 January Newsletter Subscribers 871 869 842
12/28/96 Quarterly Review Subscribers 863 861 823
12/15/96 January Newsletter draft editor@isp.com 1 1 1
12/01/96 December Newsletter Subscribers 863 859 858
11/01/96 November Newsletter Subscribers 824 824 820
10/01/96 October Madness Subscribers 811 810 810
10/01/96 October Newsletter Subscribers 811 810 810
選択
280
ヘルプ
228
158
285
次
選択：基本フォーマット毎ページ１０行受信者要約
284
Document: Done

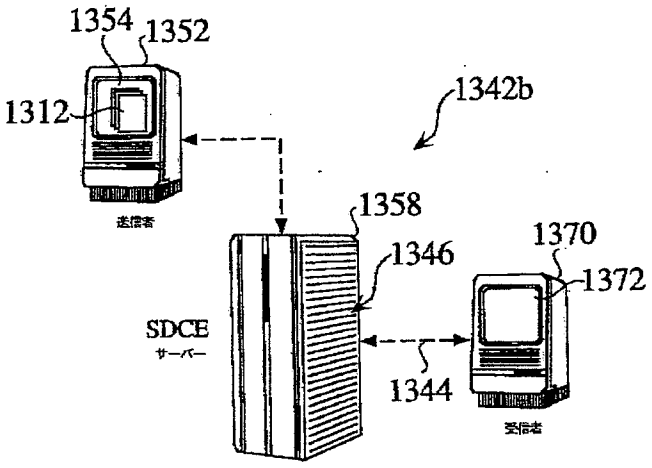
【図１６】


282
追跡レポート
162
142 144 146 148 150 152
154
156
192
224
225
226
追跡レポート
270
274
272
Packages 1-10 of 12
送信日
サブジェクト
受信者：
通知済
受信済
01/22/97 Party Invite jane@isp.com 01/22/97 01/22/97
01/22/97 Party Invite joe@isp.com 01/22/97 01/22/97
01/22/97 Party Invite dan@isp.com 01/22/97 01/22/97
01/01/97 February Newsletter draft editor@isp.com 01/01/97 01/01/97
12/28/96 Quarterly Review editor@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review jane@isp.com 12/28/96 —
12/28/96 Quarterly Review joe@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review dan@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review erik@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review louise@isp.com 12/28/96 —
レポート
選択
280
ヘルプ
228
158
285
次
選択：基本フォーマットページ毎１０行受信者詳細
284
Document: Done

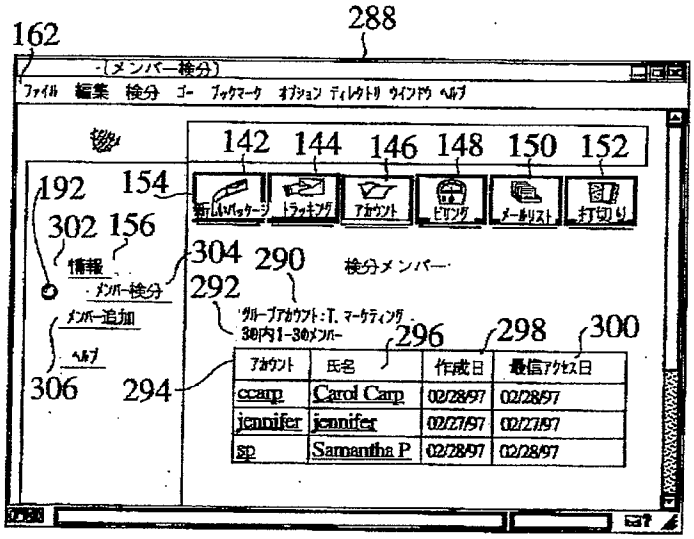
【図１７】



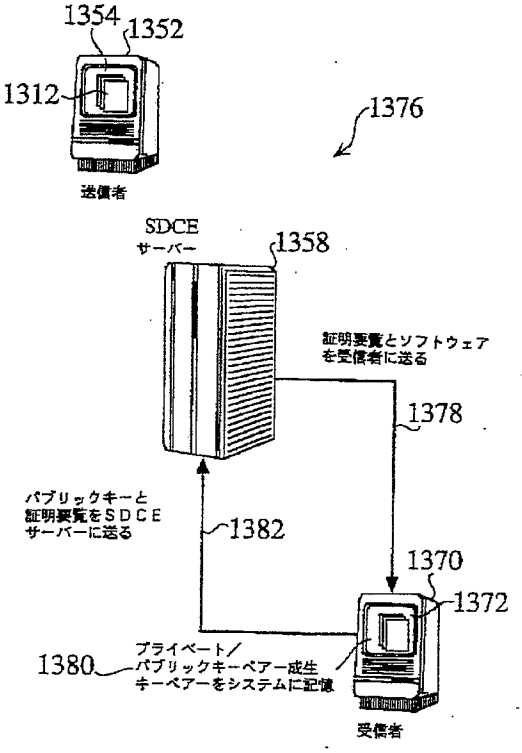
【図３２】



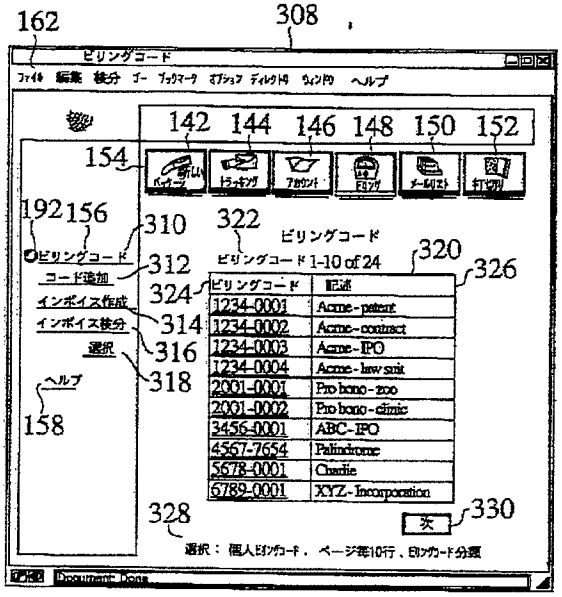
【図１８】



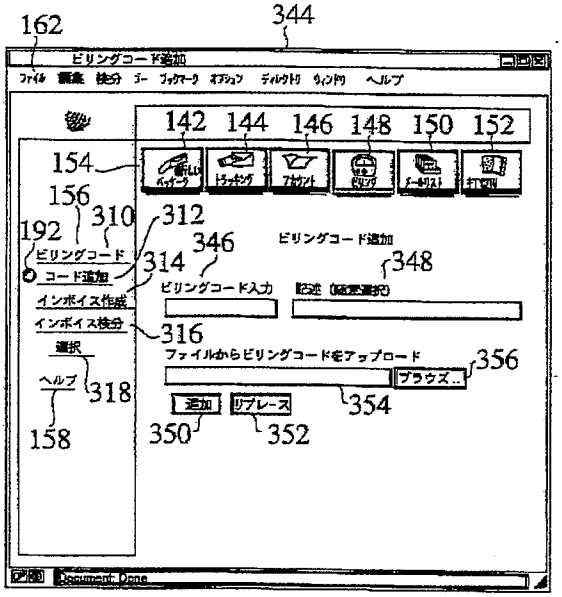
【図３９】



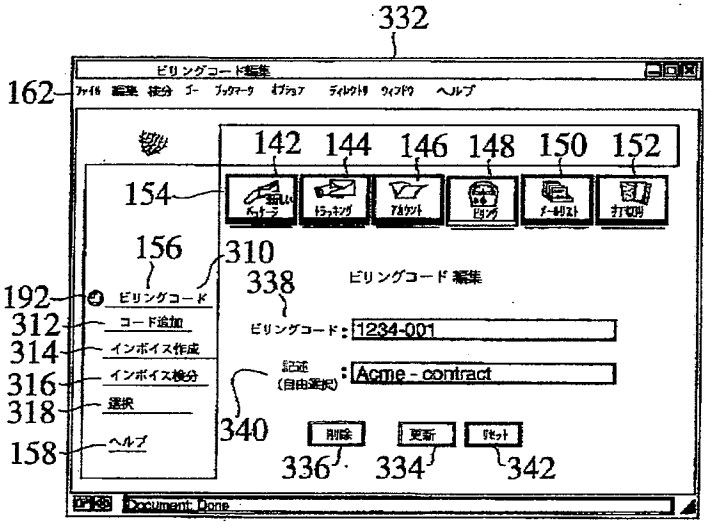
【図１９】


162
308
ビリングコード
142 144 146 148 150 152
154
192 156
310
322
ビリングコード
312
ビリングコード 1-10 of 24
320
326
コード追加
324
ビリングコード | 記述
インボイス作成
1234-0001 | Acme - patent
314
インボイス検分
1234-0002 | Acme - contract
316
1234-0003 | Acme - IPO
選択
318
1234-0004 | Acme - law suit
2001-0001 | Pro bono - zoo
ヘルプ
2001-0002 | Pro bono - clinic
158
3456-0001 | ABC - IPO
4567-7654 | Palindrome
5678-0001 | Charlie
6789-0001 | XYZ - Incorporation
328
次
330
選択： 個人ビリングコード， ページ毎10行 、ビリングコード分類
Document: Done

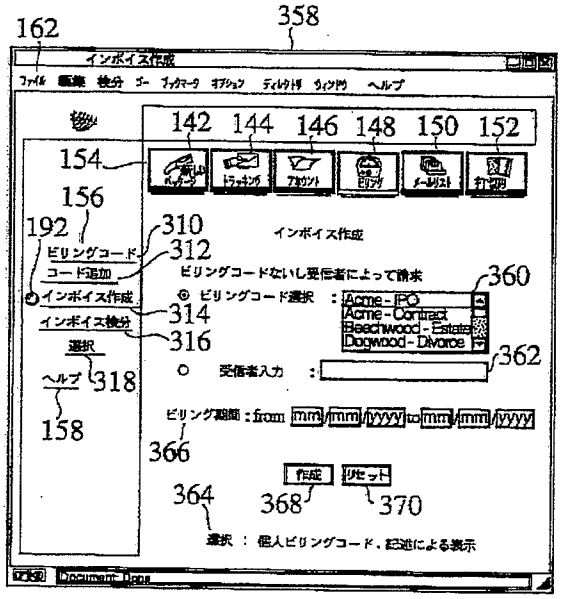
【図２１】


162
344
ビリングコード追加
142 144 146 148 150 152
154
156
192
310
312
ビリングコード
346
ビリングコード追加
314
348
コード追加
ビリングコード入力
記述 (自由選択)
インボイス作成
316
インボイス検分
ファイルからビリングコードをアップロード
356
選択
ブラウズ..
ヘルプ
318
354
追加
リプレース
158
350
352
Document: Done

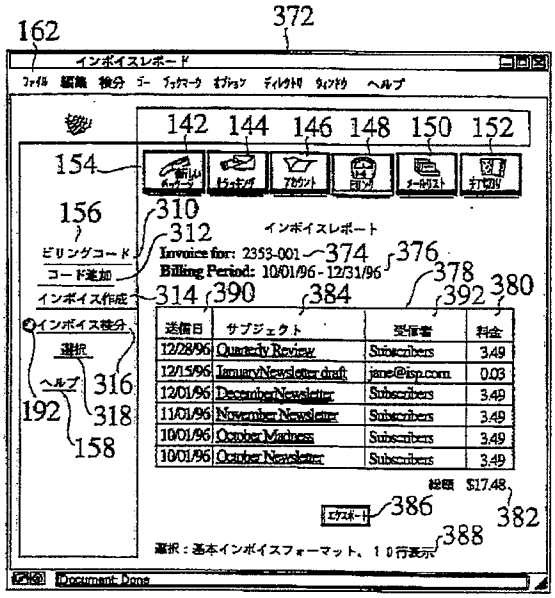
【図２０】


332
ビリングコード編集
162
142 144 146 148 150 152
154
156
310
338
ビリングコード 編集
192
ビリングコード
312
コード追加
ビリングコード: 1234-001
314
インボイス作成
記述
(自由選択)
: Acme - contract
316
インボイス検分
318
選択
340
158
ヘルプ
削除
更新
リセット
336
334
342
Document: Done

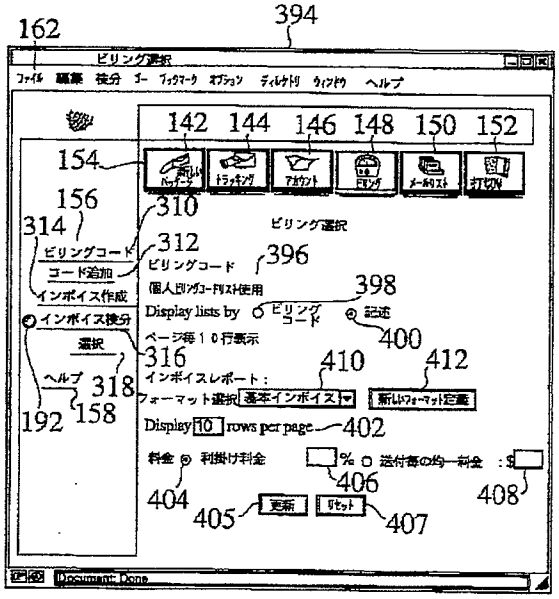
【図２２】



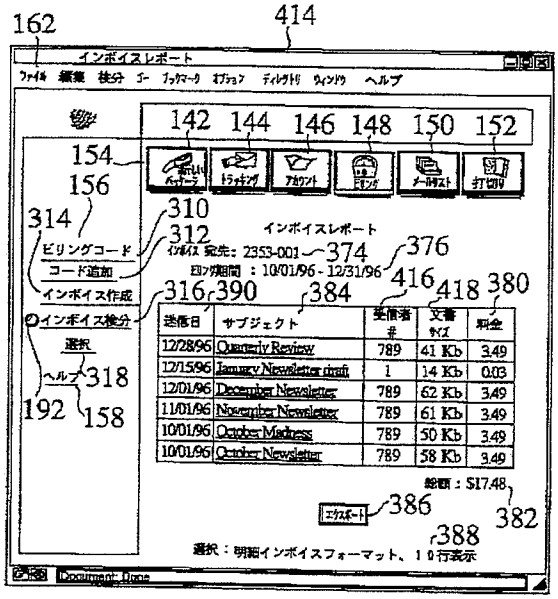
【図２３】



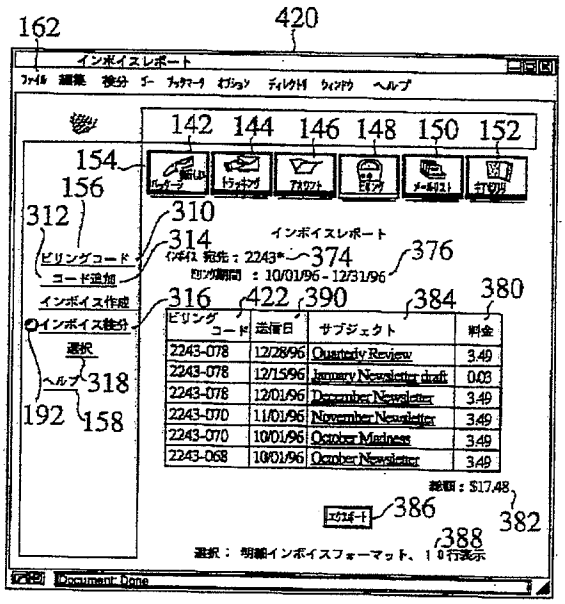
【図２４】



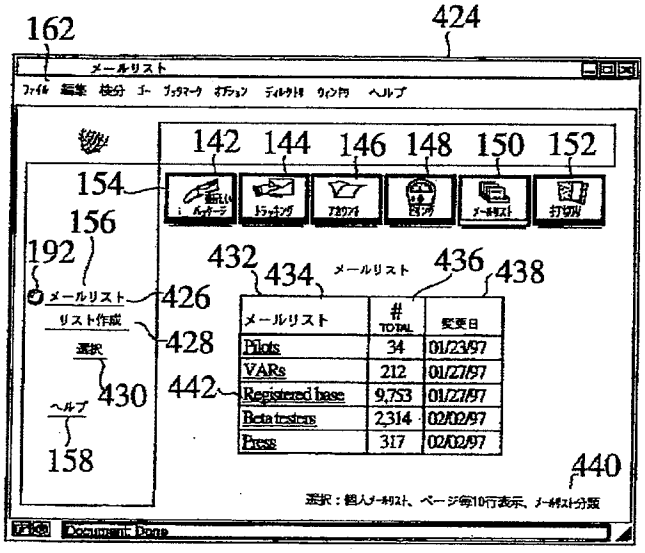
【図２５】



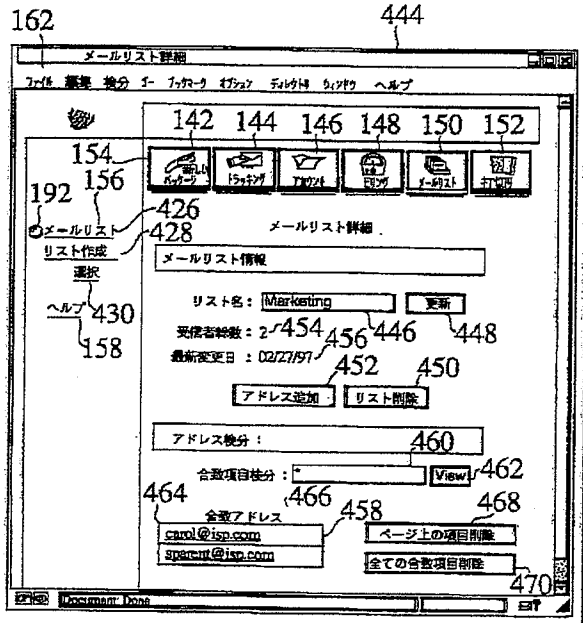
【図２６】


162
420
インボイスレポート
142 144 146 148 150 152
154
156
312
310
314
ビリングコード
コード追加
インボイス作成
インボイス検分
選択
ヘルプ
318
192
158
インボイスレポート
インボイス 宛先：2243*
ビリング期間 ：10/01/96 - 12/31/96
374
376
316
422
390
384
380
ビリングコード
送信日
サブジェクト
料金
2243-078 12/28/96 Quarterly Review 3.49
2243-078 12/15/96 January Newsletter draft 0.03
2243-078 12/01/96 December Newsletter 3.49
2243-070 11/01/96 November Newsletter 3.49
2243-070 10/01/96 October Madness 3.49
2243-068 10/01/96 October Newsletter 3.49
総額：$17.48
386
382
388
選択： 明細インボイスフォーマット、１０行表示
Document Done

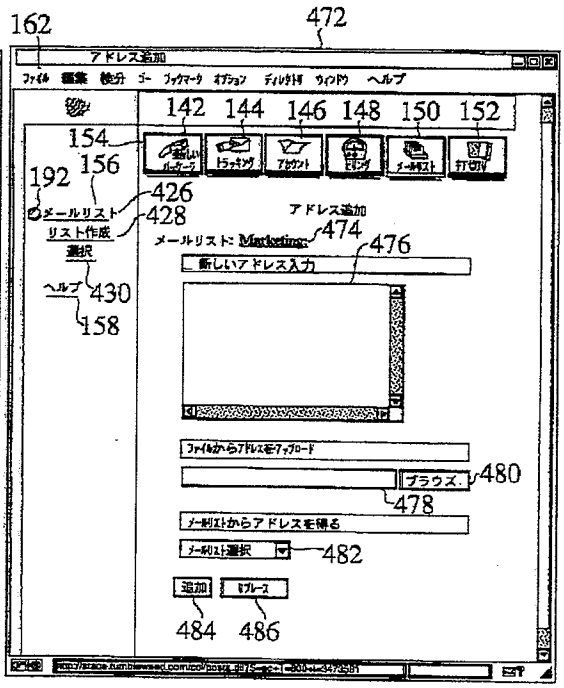
【図２７】


162
424
メールリスト
142 144 146 148 150 152
154
156
192
メールリスト
リスト作成
選択
ヘルプ
158
426
428
430
442
432
434
メールリスト
436
438
メールリスト
TOTAL
変更日
Pilots 34 01/23/97
VARs 212 01/27/97
Registered base 9,753 01/27/97
Beta testers 2,314 02/02/97
Press 317 02/02/97
440
選択：個人メールリスト、ページ毎10行表示、メールリスト分類
Document Done

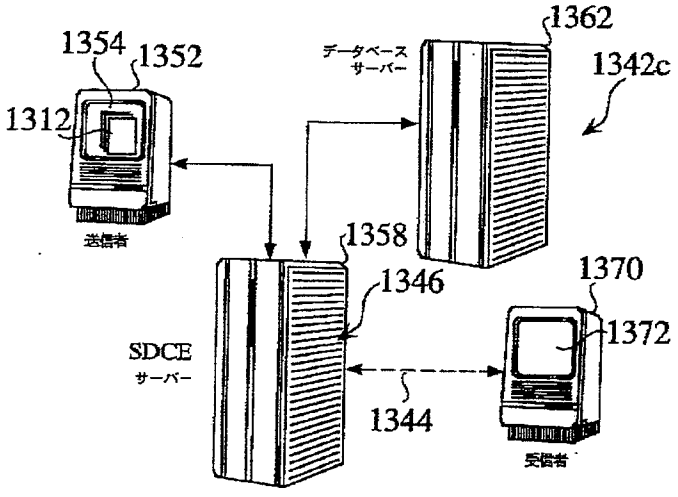
【図２８】



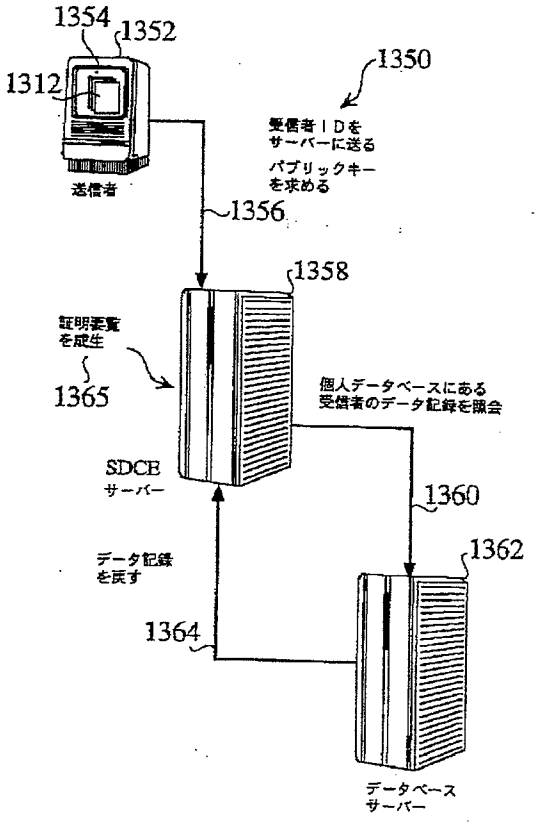
【図２９】



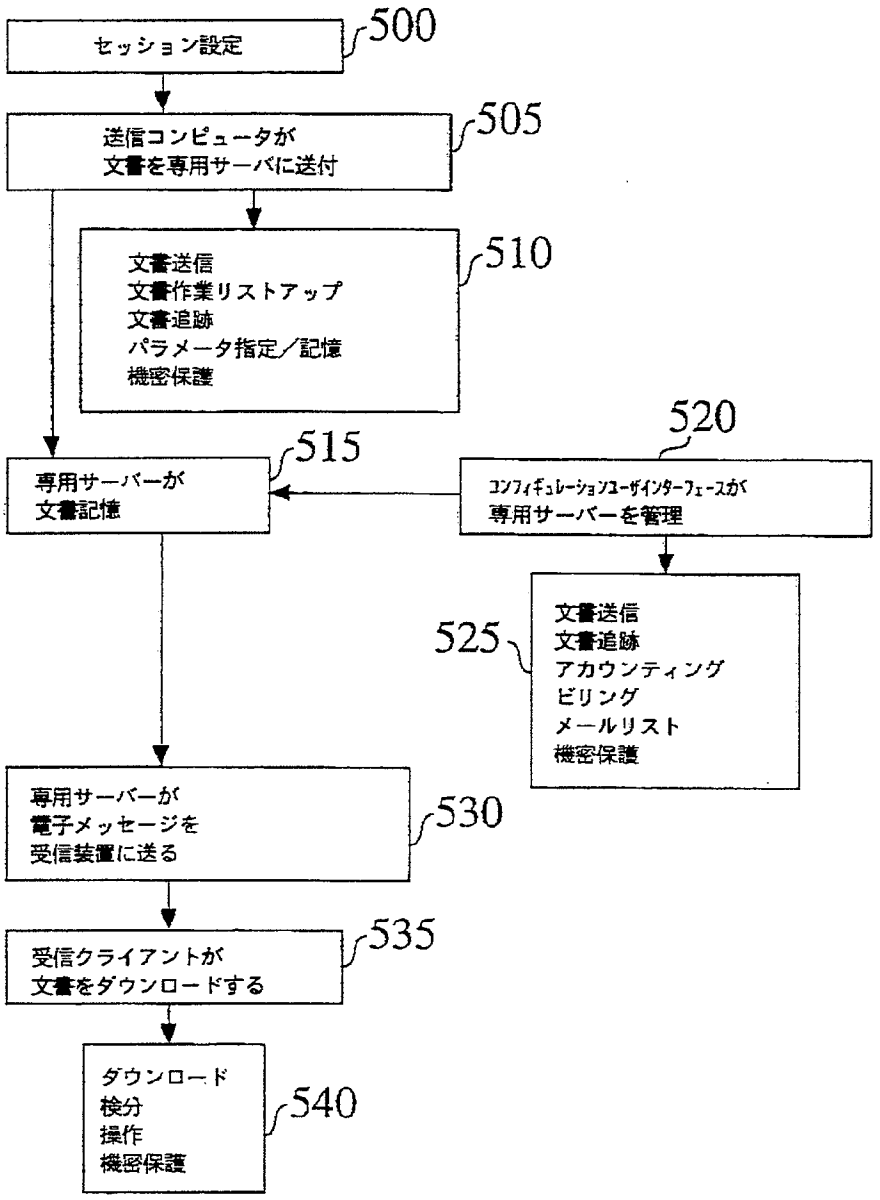
【図３３】



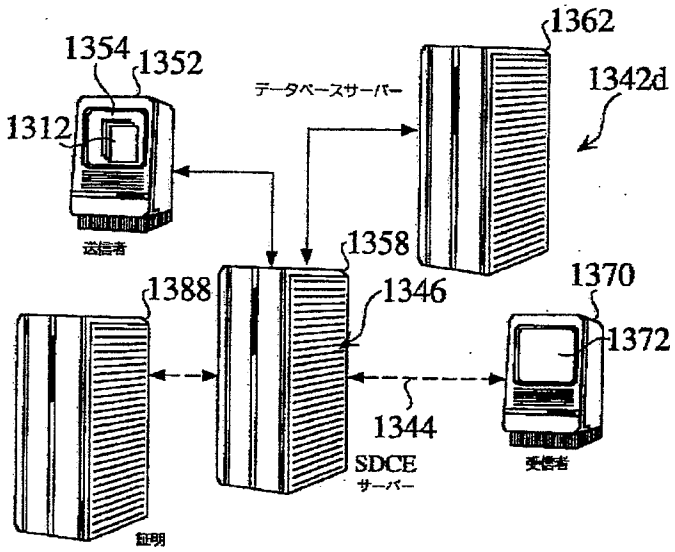
【図３７】



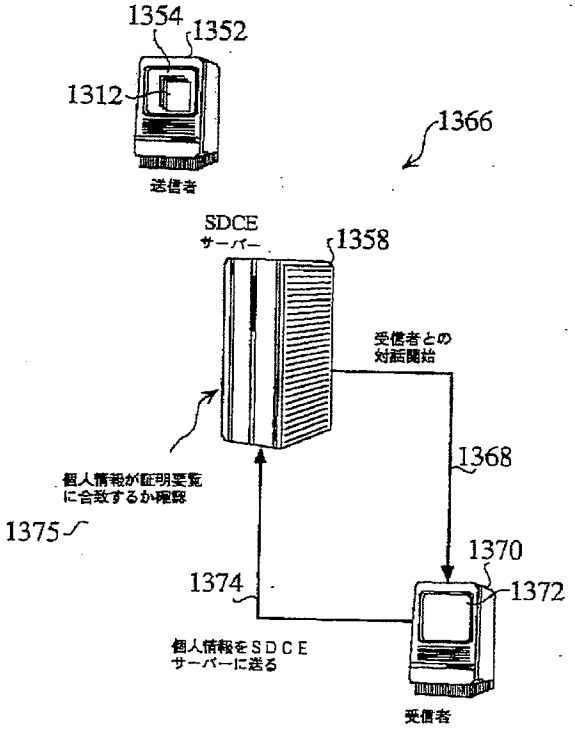
【図３０】


セッション設定
500
送信コンピュータが
文書を専用サーバに送付
505
文書送信
文書作業リストアップ
文書追跡
パラメータ指定／記憶
機密保護
510
520
専用サーバーが
文書記憶
515
コンフィギュレーションユーザインターフェースが
専用サーバーを管理
525
文書送信
文書追跡
アカウンティング
ビリング
メールリスト
機密保護
専用サーバーが
電子メッセージを
受信装置に送る
530
受信クライアントが
文書をダウンロードする
535
ダウンロード
検分
操作
機密保護
540

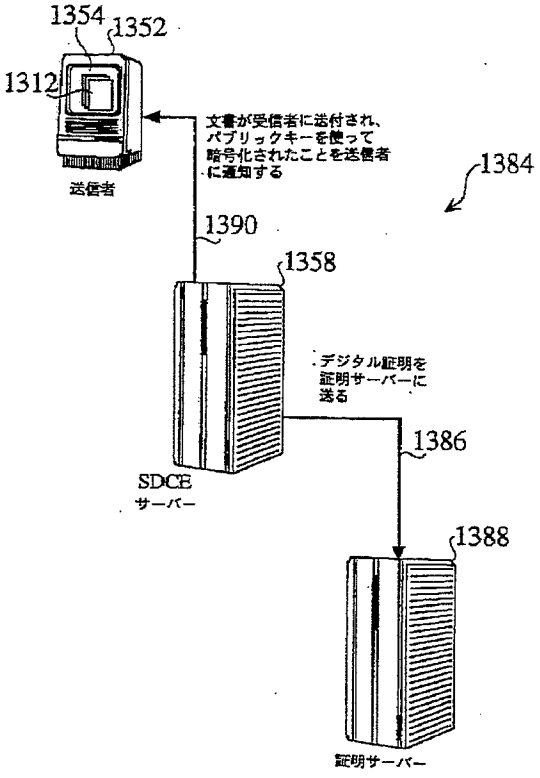
【図３４】


1362
1354
1352
データベースサーバー
1342d
1312
送信者
1358
1388
1346
1370
1372
1344
SDCE
サーバー
受信者
証明

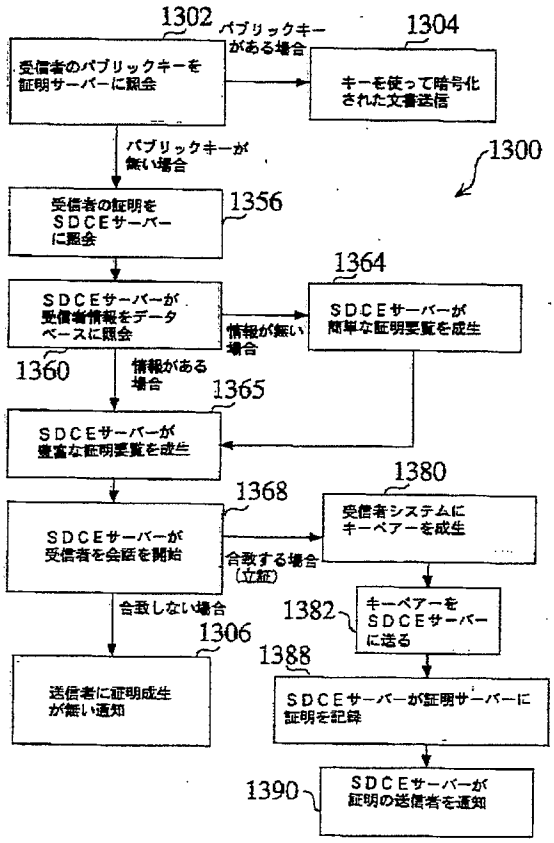
【図３８】


1354
1352
1312
1366
送信者
SDCE
サーバー
1358
受信者との
対話開始
1368
個人情報が証明要覧
に合致するか確認
1375
1370
1374
1372
個人情報をＳＤＣＥ
サーバーに送る
受信者

【図４０】


1354
1352
1312
送信者
文書が受信者に送付され、
パブリックキーを使って
暗号化されたことを送信者
に通知する
1384
1390
1358
デジタル証明を
証明サーバーに
送る
1386
SDCE
サーバー
1388
証明サーバー

【図４１】



フロントページの続き

(51)Int.Cl.[6]	識別記号	FI	
H04L 9/32		H04L 9/00	675B
12/54		11/20	101B
12/58			

(72)発明者　ジャン　クリストフ　バンディーニ
アメリカ合衆国　カリフォルニア州　95014　クーパーティノ　ノース　フットヒル　ブールヴァード　10230－イー10

(72)発明者　ランディー　シュープ
アメリカ合衆国　カリフォルニア州　94114　サン　フランシスコ　ダイアモンド　ストリート　9054

【外国語明細書】

METHOD AND APPARATUS FOR DELIVERING DOCUMENTS OVER AN ELECTRONIC NETWORK

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to communication over an electronic network. More particularly, the invention relates to a method and apparatus for delivering formatted documents over an electronic network, such as the Internet, in a secure fashion. Further, the invention relates to the field of electronic document encryption. More particularly, the invention relates to techniques for the secure delivery of electronic documents to remote recipients.

DESCRIPTION OF THE PRIOR ART

Electronic networks, such as the Internet and intranets are increasingly being used to store and distribute a variety of data. For example, a World Wide Web (Web) page may include text, graphical displays, video displays, animation, and sounds. The Web enables a recipient to receive a document from a sender, regardless of platform, operating system, or E-mail system. Such communication is possible even when the document is not received at a computer but, rather, is received at a fax machine or networked printer connected to the Internet.

In many instances, the sender of a document resides on a local area network, referred to herein as an intranet. The sender's computer may be connected to the Internet directly, or through the intranet's server. Users who do not have a direct Internet connection can subscribe to the services of an access provider, called an Internet Service Provider (ISP) in the case of the Internet.

The ISP maintains a network that connects its clients to the Internet, providing a server computer that acts as a host to its clients. The client accesses the Internet by using a computer with a modem to dial up the ISP, through the public telephone system. The ISP usually provides a point-to-point (serial) link through which the client communicates directly to the Internet, using the Internet standard TCP/IP protocols.

Existing transmission schemes are frequently not suitable for sending certain documents over, for example, the Internet. Critical documents must be sent with complete security. However, the disparate E-mail systems have varying levels of security support. It is therefore difficult or impossible to determine whether an electronic communication is secure.

Various cryptographic schemes have been used to provide security for electronic communications. However, the recipient of an encrypted message must have not only the decryption scheme, but sufficient hardware and software to decrypt the communication. Thus, it is frequently not practical or possible to send such an encrypted message.

Thus, users are often reluctant to send documents electronically. These users must rely upon the slower and more expensive methods of courier service, and conventional mail service.

It is also desirable to be able to track a critical or sensitive document to insure that it has been properly received. However, it is extremely difficult, if not impossible, to track a document from point to point along the electronic network. For example, an E-mail message sent via the Internet is broken up into many discrete data packets. The packets are sent separately through the Internet to the intended recipient. Each packet may take a different route before being re joined to form the original document and delivered to the recipient. Therefore,

tracking such document has required tracking each individual packet through each link of the Internet.

Additionally, while a computer may provide some level of security for a received document, for example, with passwords or cryptography, an electronic communication is not necessarily directed to a computer. Thus, a critical document sent electronically to a printer or a fax machine is potentially exposed to public view.

Even if such document is transmitted securely, it may not be legible when received. One problem common to E-mail is loss of document formatting. A document sent via E-mail is typically sent either as text in the body of the E-mail message, or as an attachment thereto. A text document usually does not retain the formatting of the original document. An attached document can retain formatting in some circumstances, such as if both sender and recipient have compatible software applications. However, some formatting may be lost even when the recipient opens a received document using the same application in which it was created.

Changes in document formatting can create significant problems. Electronic forms may not be compatible if their formats are different. A misformatted document may not be comprehensible to the recipient. While many formatting changes are correctable, the costs to the recipient in terms of time and expense may be substantial.

It would therefore be an advantage to provide a method and apparatus for securely delivering documents over an electronic network, such as the Internet. It would be a further advantage if such method and apparatus tracks the sending and receipt of a document. It would be yet another advantage if such method and apparatus preserves the formatting of a delivered document.

The development of computerized information sources, such as those provided through the Internet or other on-line sources, has led to a proliferation of electronically available information. The desired or required security for the secure distribution of information and documents across networks has led to a variety of architectures and techniques to protect this information.

Encryption is a basic technique to scramble information or documents to prevent unsolicited access to that information.

Figure 1 is a block diagram of secret key encryption 1210a, wherein a document 1212 is encrypted, or scrambled 1216, with a secret key 1214, producing an encrypted document 1220. The encrypted document 1220 can then be transferred to a recipient. Secret key encryption, sometimes referred to as symmetric key cryptography, employs a technique of scrambling information to prevent unsolicited access, using a unique, secret key 1214.

Figure 2 is a block diagram of secret key decryption 1210b, wherein the same, unique secret key 1214 is required to unscramble 1222 the encrypted document 1220, to reproduce a copy of the original document 1212. Without access to the secret key 1214, an encrypted document 1220 remains secure from tampering.

One potential issue with secret key encryption 1210a and 1210b is the challenge of distributing the secret key 1214 securely. For example, suppose a sender uses secret key encryption to encrypt a document 1212, and then sends a recipient the encrypted document 1220. The recipient needs the secret key 1214 to decrypt 1222 the encrypted document 1220. If the secret key 1222 is sent over a non-secure channel, then the integrity of the security is compromised. For most applications, telephone or fax provides a secure enough means of delivering secret keys 1214, while the encrypted document 1220 can be delivered over the internet using the Posta™ document delivery

system. In some instances, however, senders and recipients require a more robust or convenient means of distributing a secret key 1214.

Public key encryption facilitates a more robust, and typically a more convenient means, of delivering information securely. With public key encryption, each recipient owns a pair of keys, called a public key and a private key. The key pair's owner (the recipient) publishes the public key, and keeps the private key a secret.

Fig. 3 is a block diagram of public key encryption 1230a, wherein a document 1312 is encrypted, or scrambled 1234, with a public key 1332, producing an encrypted document 1336. To send information to a recipient, a sender uses the published public key 1332 of the intended recipient to encrypt 1234 the information, and then the recipient uses their own private key 1334 (Fig. 4) to decrypt the information. Hence, the private key 1334 (which is necessary to decrypt the information) is not distributed. Fig. 4 is a block diagram of private key decryption 1230b, wherein the private key 1334 is required to unscramble 1238 the encrypted document 1336, to reproduce a copy of the original document 1312. Without access to the private key 1334, an encrypted document 1336 remains secure from tampering.

Public key encryption 1230a and 1230b typically exploits a mathematical relationship between the public and private keys 1332, 1334, which allows a public key 1332 to be published, without risking the derivation of the private key 1334 from the published public key 1332.

Public key encryption algorithms are typically complex, and hence may be too time consuming to be of practical use for many users. Secret key encryption 1210a, 1210b is typically much faster than public key encryption 1230a, 1230b, but requires the transmission the secret key 1214 from the sender to the recipient.

In a digital envelope system, a user encrypts a document 1212 with a secret key 1214, and then encrypts the secret key 1214 with the public key 1332 of the intended recipient. The recipient of the encrypted document 1220 then uses their private key 1240 to decrypt the secret key 1214, and then uses the secret key 1214 to decrypt the document.

It is often useful to verify if a document has not been altered during transmission, or to verify who sent or received a given document. Hashing algorithms (or message digests) and public key technologies facilitate solutions to document integrity and transport verification.

Digital certificates can also be used to provide enhanced security for encrypted information. Suppose a recipient owns a public/private key pair and wishes to publish the public key 1332 so others can use the public key 1332, either to encrypt information to be sent to the recipient, or to verify the digital signature of the recipient. A secure technique for the recipient to publish the public key 1332 is to register the public key 1332 with a trusted authority. The trusted authority can then certify that a particular public key 1332 belongs to the recipient. A digital certificate connects a recipient, or other entity, with a particular public key 1332.

A digital certificate, as disclosed later, is a record of a public key and an identity, and the association of the two as attested to by a third party by means of a digital signature. The private key is not in the certificate, but only one private key can match a given public key. A public/private key pair is actually a pair of numbers with the following properties:

The private key cannot be derived easily from the public key; and

The public key can be used to cipher data which can only be deciphered by knowing the private key (some public keys algorithms, such as RSA, also have the inverse property, which makes them suitable for use a digital signatures).

A trusted or certificate authority issues and maintains digital certificates.

The disclosed prior art systems and methodologies thus provide some methods for the encryption and secure delivery of documents, but fail to provide a simple digital certificate generation and enrollment system that is implemented and controlled by a sender. The development of such a digital certificate system would constitute a major technological advance.

SUMMARY OF THE INVENTION

The invention provides a method and apparatus for securely delivering documents over an electronic network. The invention permits a user to track the sending and receipt of a document, while preserving the document's original formatting.

For the purposes of the discussion herein, the term "document" includes any contiguous collection of data, including a stream of data, video data, audio data, animation, a platform-independent formatted document such as an HTML, PDF, or Envoy document, a platform-specific formatted document such as a Microsoft Word or Excel document, an unformatted document such as a text document, a custom-generated report or Web page, or a grouping of one or more database records, such as SQL records. The term document can also include a grouping of one or more such documents. While the preferred embodiment of the invention is adapted for use in document transmission over the Internet, the invention is equally applicable to other wide area or local area networks.

In accordance with a presently preferred embodiment of the invention, a send client application is provided that allows a user to send a document over an electronic network from the desktop of a sending computer. Such document may also be sent from within a document authoring application.

A dedicated server is provided to store the document received from the sending computer. The dedicated server then forwards an electronic message to a receiving device to notify the recipient of the document's transmission.

The intended recipient downloads the stored document from the dedicated server in response to this message. In the preferred embodiment of the invention, the receiving device is a personal computer. However, in alternate embodiments, the receiving device includes a network server device, fax machine, printer, Internet-compatible telephone, Internet access appliance, or personal digital assistant.

A receive client application provided on the receiving device is used to download the document from the dedicated server. The receive client application is preferably a Web browser, but can be any other software application capable of retrieving the stored document while preserving document formatting. The receive client application permits the recipient to receive, view, print, and manipulate the document.

The send client application is accessed via an application window. The application window is displayed on the sending computer's desktop. The application window includes a persistent tool bar for accessing main functions and a menu listing operational commands for the send client application.

A package manager and a package window are also accessed from the application window. The package manager lists all document activities initiated during an application session. The package window allows the user to specify

parameters of the document delivery, including the recipient(s), the document(s), and send options. Document delivery parameters may be stored in a storage module for later modification and/or use.

A document is specified for delivery in several ways. The user can click and drag the document from the sending computer desktop onto one of the application window or the package window. The document may also be dragged onto either the icon representing the send client application or the icon for accessing the stored document delivery parameters. The user can also browse local and network directories and select desired documents. A document can also be sent from within a document authoring application.

A configuration user interface (CUI) is provided for directly invoking and customizing the dedicated server. In the preferred embodiment of the invention, the CUI is an HTML interface. The dedicated server is therefore directly invoked and customized via a Web browser. This HTML interface includes modules for sending and tracking the document, accessing account information, managing billings, and managing mail distribution lists.

The CUI is accessed via a CUI application window displayed on a managing computer desktop. The managing computer can be the sending computer, the receiving computer, the dedicated server, or some other entity in the electronic network. The CUI application window displays a main tool bar for accessing main functions, and a secondary tool bar for accessing secondary functions. The CUI application window also includes a workspace for displaying an interactive interface to an accessed function, and a menu listing operational commands.

The invention also provides a security framework that restricts system access to an authorized user. The types of security supported include authentication layers, secure socket layers, password protection, private key encryption, public

key encryption, and certificate authentication. The security framework can be implemented as one or more modules, and can be incorporated into at least one of the send client application, the receive client application , and the CUI.

A sender driven certificate enrollment system and methods of its use are provided, in which a sender controls the generation of a digital certificate, which can be used to encrypt and send a document to a recipient in a secure manner. The sender compares previously stored recipient information to gathered information from the recipient. If the information matches, the sender transfers key generation software to the recipient, which produces the digital certificate, comprising a public and private key pair. The sender can then use the public key to encrypt and send the document to the recipient, wherein the recipient can use the matching private key to decrypt the document. In a preferred embodiment, a server is interposed between the sender and the recipient, to provide increased levels of system security, automation, and integrity.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram of secret key encryption of a document;

Fig. 2 is a block diagram of secret key decryption of a document;

Fig. 3 is a block diagram of public key encryption of a document;

Fig. 4 is a block diagram of private key decryption of a document;

Fig. 5 is a diagram of a document delivery system according to the invention;

Fig. 6 is a view of an application window according to the invention;

Fig. 7 is a view of an application window showing document activities according to the invention;

Fig. 8 is a view of a package window, according to the preferred embodiment of the invention;

Fig. 9 is a view of a recipient's window according to the invention;

Fig. 10 is a view of a CUI application window according to the invention;

Fig. 11 is a view of a CUI package window according to the invention;

Fig. 12 is a view of a CUI options page according to the invention;

Fig. 13 is a view of a CUI tracking search page according to the invention;

Fig. 14 is a view of a CUI tracking report preferences dialog according to the invention;

Fig. 15 is a view of a recipient summary tracking report in basic format according to the invention;

Fig. 16 is a view of a recipient detail tracking report in Basic Format according to the invention;

Fig. 17 is a view of a recipient detail tracking report in billing code format according to the invention;

Fig. 18 is a view of a group account manager account - view members window according to the invention;

Fig. 19 is a view of a billing codes window according to the invention;

Fig. 20 is a view of an edit billing codes dialog according to the invention;

Fig. 21 is a view of an add billing codes dialog according to the invention;

Fig. 22 is a view of a create invoice page, according to the invention;

Fig. 23 is a view of a basic invoice report window according to the invention;

Fig. 24 is a view of a billing preferences dialog according to the invention;

Fig. 25 is a view of an invoice report in spec invoice format according to the invention;

Fig. 26 is a view of an invoice report in billing code invoice format according to the invention;

Fig. 27 is a view of a mail list page according to the invention;

Fig. 28 is a view of a mail list detail page according to the invention;

Fig. 29 is a view of an add addresses page according to the invention; and

Fig. 30 is a flow chart of the method for delivering a document over an electronic network according to the invention.

Fig. 31 shows a basic certificate enrollment system implemented between a sending computer and a receiving computer across a network;

Fig. 32 shows a certificate enrollment system implemented between a sending computer, a SDCE server and a receiving computer;

Fig. 33 shows a certificate enrollment system implemented between a sending computer, a SDCE server, a database server and a receiving computer;

Fig. 34 shows a certificate enrollment system implemented between a sending computer, a SDCE server, a database server, a certificate server and a receiving computer;

Fig. 35 is a block diagram of a digital certificate;

Fig. 36 is a block diagram of a certificate digest;

Fig. 37 shows the first stage of operation for the sender driven certificate enrollment system;

Fig. 38 shows the second, attestation conversation stage of the sender driven certificate enrollment system;

Fig. 39 shows the third, public/private key pair generation stage of the sender driven certificate enrollment system;

Fig. 40 shows the fourth stage of the sender driven certificate enrollment system, referred to as forwarding and registration of the receiver public key; and

Fig. 41 is flow chart that shows the basic decision tree for the sender driven certificate enrollment system.

DETAILED DESCRIPTION OF THE INVENTION

The invention provides a method and apparatus for securely delivering a document over an electronic network. The invention provides a user with the ability to track the sending and receipt of such document. Throughout the delivery, the formatting of the document is preserved.

For the purposes of the discussion herein, the term "document" includes any contiguous collection of data, including a stream of data, video data, audio data, animation, a platform-independent formatted document such as an HTML, PDF, or Envoy document, a platform-specific formatted document such as a Microsoft Word or Excel document, an unformatted document such as a text document, a custom-generated report or Web page, or a grouping of one or more database records, such as SQL records. The term document can also include a grouping of one or more such documents. While the preferred embodiment of the invention is adapted for use in document transmission over the Internet, the invention is equally applicable to other wide area or local area networks.

The display screens and configuration of the graphical user interface described below are provided in accordance with the presently preferred embodiment of the invention. However, one skilled in the art will appreciate that such display screens and graphical user interfaces are readily modified to meet the requirements of alternative embodiments of the invention. The following discussion is therefore provided for purposes of example and not as a limitation on the scope of the invention.

Fig. 5 is a diagram of a document delivery system 10 according to the invention. The system allows the user to send a document 16 or set of documents and a recipient address or set of recipient addresses from the desktop 12 of a sending computer 14 over an electronic network 18 using a send client application 20. Such document may also be sent from within a document authoring application,

such as a word processor, spreadsheet, or graphics application. The send client application is preferably stored on the sending computer, but may be stored in a remote location accessible to the sending computer.

The sending computer connects to a dedicated server 22. The dedicated server functions in accordance with such standards as, for example Internet standards to manage the transfer of documents between senders and recipients. The dedicated server may be a server provided by an Internet service provider (ISP), or may be a separate dedicated server.

In the preferred embodiment of the invention, documents are uploaded to, and downloaded from the dedicated server using the hypertext transport protocol (HTTP). HTTP is the communications protocol used to connect to servers on the World Wide ("Web"). A significant advantage of HTTP is that it is application and platform-independent. Thus, the sender and recipient do not need to use the same Web browser, or even the same operating system.

The dedicated server 22 stores the document received from the sending computer 14. The dedicated server then forwards an electronic message to a receiving device at the address received from the send client application to notify the intended recipient of the document's transmission. This notification message is sent as a text (e.g. ASCII) message using the simple mail transport protocol (SMTP) of the Internet.

In the preferred embodiment of the invention, the receiving device is a personal computer 24. However, in alternate embodiments, the receiving device may include a printer 26, fax machine 28, network server device, Internet-compatible telephone, Internet access appliance, or personal digital assistant (not shown).

The notification message contains the uniform resource locator (URL) of the document, which allows the server to locate the document. In response to this

message, the intended recipient downloads the stored document from the dedicated server 22 with a receive client application 30. The receive client application is preferably stored at the receiving device, but may be stored in a remote location that is accessible to the receiving device. The receive client application permits the recipient to receive, view, print, and/or manipulate the document.

In the preferred embodiment of the invention, the receive client application is a Web browser. Thus, the intended recipient can copy the URL directly from the notification message, and paste it into a Web browser on the receiving computer. The Web browser then retrieves the document from the dedicated server. In alternative embodiments of the invention, the receive client application is any other software application capable of retrieving the stored document from the dedicated server while maintaining document formatting.

The send client application is readily installed on a computer from a CD-ROM, or by downloading from the Web. For example, a user who already has an account with a dedicated server provider can configure the send client application with the appropriate account information. A user who does not have such an account is directed to a URL that has the information for setting up an account.

The send client application is accessed via an application window displayed on the sending computer's desktop. The application window is displayed once the account information is properly configured. Fig. 6 is a view of an application window 32, according to the preferred embodiment of the invention.

The main function of the application window is to view the status of, and to manage send client application activity. The application window also serves as a launching pad to reach the various functions of the send client application and the configuration user interface CUI (discussed below).

In the preferred embodiment of the invention, the application window displays a main tool bar 34 for accessing main functions of the send client application. One such function is the selectable button for new package 36. Clicking on new package opens a new package window (discussed below), which allows a user to initiate a delivery of a document. Clicking on the open button 38 opens either a saved delivery parameter or a saved package window (discussed below).

In the preferred embodiment, the main tool bar 34 includes buttons that are Internet shortcuts to CUI functions. Clicking on such button launches the user's Web browser and displays the appropriate page in the CUI. In the preferred embodiment of the invention, no additional login is required in this process. Examples of such buttons include tracking 40, account 42, billing 44, and mail lists 46 buttons.

Buttons may also be provided for send client application settings. For example, a preferences dialog accessed via a setup button 48 permits the user to specify dedicated server and proxy server account information. The user can also specify whether or not to use a low-level secure communications protocol, such as Secure Socket Layer (SSL) to secure the connection between the desktop and the dedicated server for all transmissions.

The send client application can access the local address books of supported applications. In the preferred embodiment of the invention, the user selects the setup button 48 and is presented with a pull-down menu which lists the address books supported by the invention. The user then selects the desired address book file.

A stop button 50 is used to stop transmission of all information to the dedicated server. In the preferred embodiment of the invention, once clicked, the stop

button remains depressed. To resume transmission, the user clicks on the button again, and it returns to a raised position.

The menu 52 lists operational commands for the send client application. In the preferred embodiment of the invention, the file menu 54 contains commands that have the same functionalities as buttons on the main tool bar 34. Other commands provide information regarding the send client application, or are Internet shortcuts to functions of the CUI. In Fig. 6, the menu includes listings for edit 56, package 58, CUI 60, and help 62.

The application window also displays a package manager 64 that lists all document activities initiated during an application session. The package manager is an area, or set of fields in the body of the application window which lists all document activities that have been initiated during a send client application session. When the send client application is first launched, the package manager field is empty. However, as documents are sent, they are listed in the package manager.

Fig. 7 is a view of an application window 32 showing document activities 72 according to the preferred embodiment of the invention. The package manager may display the recipient(s) 66, the subject 68, and the status 70 of the delivery. The status of an active delivery may be represented as a dynamic percentage of upload completed. Other possible status labels include "completed," "error," "pending," and "on hold."

Documents may be listed, for example, in processing, or reverse processing orders. In the preferred embodiment of the invention, the document currently being processed 74 is presented in bold characters. In alternate embodiments, the current document is indicated by other means, including highlighting, flashing, or color, or is unmarked.

Clicking on a listed document 76 highlights that listing and selects the document. Multiple documents may be selected at one time. Once a document is selected, the user can use the menu 52, for example, to hold, edit, or delete the document.

A hold prevents a pending document from being processed. The document is held in a queue until it is deleted or the hold is removed. In the preferred embodiment of the invention, any or all documents in the list can be deleted. A current send is completely aborted, and an already-processed document is deleted from the window.

Editing opens a document within a new package window (discussed below). The user can then edit the document and re-submit it for sending. If a document is edited in transmission, the transmission is aborted. The document is opened in a new package window, and the next pending document is transmitted.

Fig. 8 is a view of a package window 78 according to the preferred embodiment of the invention. The package window allows the user to specify parameters of the document delivery. A new package window is accessible from the application window, for example, by menu or tool bar selections. A package window may be saved and opened at a later time. Additionally, a package window is opened when a user sends (prints) a document from a document authoring application to the send client application.

Each document delivery transaction requires the sender to specify the recipient(s) of the delivery, the document(s) to be delivered, and the delivery options. Such delivery options include priority 80, request confirmation 82, document expiration 86, scheduled notification 88, and billing code 90. The preferred embodiment of the invention includes selectable buttons such as clear form 92, save form 94, save parameters 96, and send 98.

Any number of recipients or mail lists for a given delivery are specified in the "To:" field 110 of the package window. Each recipient must be specified by an E-mail address, alias, or mail list. The user may type an address directly into the "To:" field. Alternatively, the user may access a recipients window by clicking on the "To:" button 108.

The subject of the message is entered into the subject field 134. The message itself is entered into the message field 136. The subject 134 and message 136 fields are optional. In the preferred embodiment of the invention, the subject appears in the E-mail notification message and on an HTML cover page for the downloaded document. The message appears only in the E-mail notification.

The documents field 112 in the package window allows the user to specify any number of documents to be delivered. A document is specified in several ways. The user can click and drag the document from the sending computer desktop onto one of the application window, the package window, or onto either the icon representing the send client application, or the icon for accessing the stored document delivery parameters.

Clicking the documents button 84 in the package window allows the sender to browse local and network directories and select desired documents. If the package window is invoked from a document authoring application, the document field is automatically filled in with the current active document.

A file format field 138 allows the user to specify in what electronic format the document is saved. The send client application is readily adapted to support different formats, such as Mac Binary, Envoy, PDF, Dynadoc, and HTML. For example, a document created in a word processing application operable on one platform can be saved in the format of another word processing application operable on a different platform.

Each delivery transaction has associated send options. In the preferred embodiment of the invention, all options have default settings which can be changed by the user prior to delivery. Settings are viewed and edited in the package window.

In the priority field 80, a user specifies the priority of a delivery, for example, as normal, low, high, or urgent. Priority determines the order the document is processed by the client as well as by the dedicated server.

The request confirmation field 82 is used to prompt the recipient to confirm whether or not a document was successfully received. Request confirmation can be selected or de-selected, as desired.

The security dialog 101 allows the user to specify varying levels of advanced security measures. These levels include specifying a password 100 for basic password protection, or requesting confirmation of a password 102. Additional security provisions, such as encryption 104 or requiring the recipient to use SSL to receive 106 the document, can also be provided. If the user requires the recipient to use SSL and is not using a secure connection between the sending computer desktop and the dedicated server, the recipient is asked whether or not to secure the connection to the dedicated server.

The document expiration field 86 allows the user to specify how long a document will remain on the dedicated server for recipient availability. A default, such as ten days after notification is sent, may be provided.

The scheduled notification field 88 allows the user to specify a future date and time that the dedicated server will notify the user of a given delivery. The billing codes dialog 90 allows the user to select an optional billing code from a list associated with the user's send client application account. In the preferred embodiment of the invention, a cached list of billing codes is available. A

refresh button 114 refreshes the list with the latest billing code list on the dedicated server.

Once the user has specified delivery parameters in the package window, the user initiates the document delivery by clicking the send button 98. A delivery is initiated only if both the recipient and the document fields are entered correctly. The send button is not active until both such fields are complete. If the user is working off-line, sent documents are queued for sending when the connection is eventually established.

Addresses are matched first against the current local address book. If the addresses are still not matched, they are uploaded to the dedicated server as is. The dedicated server then attempts to match addresses with a mail list. If the address is still not matched, the dedicated server appends the domain name of the account holder.

A partially completed package window may be canceled or saved using the save form button 94. The saved package window may then be re-opened for future use.

Saved delivery parameters can be used on a recurring basis across sessions. From a package window, a user can save delivery parameters including specified send options, an address list, and/or a fixed subject or message. To save delivery parameters, a user clicks on the save parameters button 96. A dialog box prompts the user to specify a name and location for the delivery parameters to be saved.

If the saved delivery parameters contain an address list, the user can initiate a delivery by clicking and dragging a document icon onto the saved delivery parameter icon. The document provides the remaining information required for

a delivery, and the send is initiated automatically. The saved delivery parameter thus serves as a dedicated mail chute to a specific set of recipients.

The existing send options may be modified or confirmed before launching the delivery. A window displaying all send parameters is opened, and the user can modify parameters or append a message before sending the document. In the preferred embodiment of the invention, the user is prompted to save any modifications to send options or existing address lists upon closing the package window.

If the saved delivery parameters do not include an address, clicking and dragging a document onto the saved delivery icon opens a package window. The saved send options and name of the document are specified in the package window. The user must specify a recipient before the document can be sent.

Saved delivery parameters are opened by clicking on the associated icon, or by selecting the appropriate main tool bar 34 or menu items. The settings are displayed in a package window and are completed or modified for a delivery. If the send client application is not open, opening the saved delivery parameters opens the application window as well as a package window. Modifications to the saved delivery parameters are preserved by replacing the existing saved parameters, or by creating a new saved delivery parameters file under a different name.

If unsaved changes have been made to the saved delivery parameters, the user is prompted to save the changes upon closing the package window. A sender can add an address list to an existing saved delivery parameter that did not previously contain an address list. The settings of the package window are saved using the "save settings as default" button 116.

Fig. 9 is a view of a recipients window according to the preferred embodiment of the invention. The recipients window 118 is used to select the recipient's name from an address book or pre-defined mail list.

In the preferred embodiment of the invention, a pull-down menu 120 allows the user to access addresses in a local address book or a mail list. For example, selecting mail list in the pull-down menu and clicking on the refresh button 122 populates the list box 124 with the names of the mail lists stored on the dedicated server for the account for which the send client application is configured. Selecting local address book and clicking on the refresh button populates the list box with addresses from the address book specified in the preferences dialog.

Each time the recipients window is opened, the send client application displays a previously cached list of addresses. Clicking on refresh forces a refresh of the list from the appropriate source. The send client application presents the last selected source for the next send, both within and across sessions. The cancel button 135 cancels the recipients window display.

A user can select items from the list box 124 and click the "To" arrow button 126 to specify the selections as recipients. In the preferred embodiment of the invention, control-click allows selection of multiple items and shift-click selects a range of items. Recipients are presented in the recipients box 128. Recipients listed in the recipients box list are selected and removed by clicking the delete button 130 or by hitting keyboard backspace or delete keys.

When the user clicks on the "OK" button 132, items in the recipients box list are displayed in the "To:" field 110 of the package window 78 (see Fig. 8). In the preferred embodiment of the invention, mail lists have the prefix "list:" prepended to them. A user can also delete or modify recipient addresses from the "To:" field of the package window.

The specified document delivery parameters may be stored in a storage module for later modification and/or use. In the preferred embodiment of the invention, the send client application and the package window are accessed by selecting their representative icons (not shown) from the sending computer's desktop.

A configuration user interface is provided for directly invoking and customizing the dedicated server. The CUI is accessed via a CUI application window displayed on a managing computer desktop. Alternatively, the CUI is accessed through any Web browser application that supports tables, or accessed through the send client application. Fig. 10 is a view of a CUI application window 140 according to the preferred embodiment of the invention.

In the preferred embodiment of the invention, the CUI is an HTML interface for invoking and customizing the dedicated server via a Web browser. This HTML interface includes modules for sending the document, tracking the document, accessing information associated with the document delivery account, managing billings for the document delivery, and managing mail distribution lists.

The CUI offers different sets of functions, depending on the user and type of account used. Individual account holders, group account managers, and group members see slightly different interfaces and are able to access and manipulate varying sets of data. When a user initiates a CUI session, the type of account is identified by the dedicated server. The specific user is then provided with the appropriate functions and data.

In the preferred embodiment of the invention, individual account holders and group account managers have access to all delivery and account information associated with the account. Account managers therefore have access to information regarding activities of all group members using the account.

Account managers are additionally authorized to create and manage member accounts. Group members have access only to information regarding the members own delivery services.

The managing computer can be the sending computer, the receiving computer, the dedicated server, or some other computer in the electronic network. The CUI includes five main functions, new package 142, tracking 144, account 146, billing 148, and mail lists 150.

In the preferred embodiment of the invention, these main functions are displayed as selectable buttons 142, 144, 146, 148, 150 on a persistent main tool bar 154. In Fig. 10, this main tool bar is displayed in a horizontal orientation, and also includes a quit button 152. However, alternative embodiments display different configurations of the application window.

A secondary tool bar 156 is provided for accessing and navigating secondary functions 164 within the main functions. In Fig. 10, the secondary tool bar is displayed in a vertical orientation. However, this configuration is for exemplary purposes only. The invention may be implemented readily to display different orientations of the main and secondary toolbars.

The secondary navigation on the secondary tool bar 156 for the CUI application window 140 includes address 166 and options 168. A help button 158 included on all secondary toolbars is used to access on-line help for the current function.

The CUI application window also includes a workspace 160 for displaying an interactive interface to an accessed function. A menu 162 lists operational commands for the CUI.

A send function mirrors that of the send client application. The send function is accessed from the new package button 142. This send function allows users to

send documents from remote locations using any browser. The send function also allows documents to be sent from platforms not supported by the send client application. In the preferred embodiment of the invention, saved delivery parameters, Envoy conversion, and access to local address books are not available.

Clicking on the new package button to access the send function brings up the package window. Fig. 11 is a view of a CUI package window 170, according to the preferred embodiment of the invention. The current function is indicated by an item 192 in the secondary tool bar.

For a given delivery, a user can manually enter names into the "To:" field 172. A mail list may also be selected from a pull-down menu 174. The user may thereby view and manipulate mail lists. In the preferred embodiment of the invention, the user does not have access to a local E-mail address book.

If an item entered in the "To:" field 172 does not contain proper domain formatting (e.g. the "@" is omitted), the item is compared to the mail lists by the Server. If the item is not located in a mail list, the server appends the sender's domain name to the end of the item.

A sender inputs text into the subject 176 and message 178 fields. The sender may specify a document to be sent by typing the name of, and path to the document into the "Document:" field 180. Alternatively, the document may be specified by clicking the browse button 182 and browsing to select a document from a local or network directory.

To send multiple documents, the sender clicks on the "Add more documents..." link 184. The sender is then presented with a window (not shown) having the same format as the new package window, with the addition of four additional "Document:" fields and browse buttons. The information already entered on the

previous CUI package window 170 is carried over into the new window. Thus in the preferred embodiment, a sender may specify up to five documents. In alternative embodiments, any number of documents may be specified.

The reset button 186 clears all fields in the window to their defaults. The send button 188 is used to initiate the delivery of the document with the default options. If the information input into the address form is incomplete or incorrect, the invention displays an error page (not shown) to the sender. The invention may also prompt a sender for a document's mimetype if it is not recognized. A mimetype specifies the format of a document, and is used by the recipient browser to bring up the corresponding application to display the document. In the preferred embodiment, the error page is directly edited, and the new information directly submitted. When the send is complete, a notification page (not shown) is displayed to the sender.

In the preferred embodiment of the invention, the CUI includes most of the send options of the send client application (see Fig. 8). These send options are accessed by clicking on the options button 190 to open a CUI options page. Fig. 12 is a view of a CUI options page 194 according to the preferred embodiment of the invention. Such options include priority 196, request confirmation 198, document expiration 200, and scheduled notification 202. However, because the send client application driver is not available from the server, certain send client options such as document type are not implemented. A document is therefore sent in the document's original format only.

A security function 204 is incorporated into the preferred embodiment of the invention. The preferred embodiment of the invention supports security and encryption features permitted under current law for use in the United States. Alternative embodiments of the invention comply with any security and encryption requirements for software applications intended for export from the United States.

The CUI user may specify a password 206 that a recipient must provide to access a document. The user may also specify confirm password 208, encrypt document 210, and require SSL to receive 212. The password may be used as a secret key to encrypt the document on the server. This provides a higher level of security while the document is stored on the server. If the encrypt document function 210 is selected but the user has not specified a password, the CUI transmits an error message when the user attempts to apply the settings.

The billing code option 214 allows users to select a billing code, including "None" from a pull-down menu. The list is defined and maintained in the billing module of the CUI (see Fig. 19). The "Billing Code" text link brings users to the billing section of the CUI. Users may thereby view and manipulate billing codes.

Clicking on the reset button 216 restores the default settings. Alternatively, the current settings may be saved 218 as the default. Once the options are set, the user uses the Update button 220 to return to the package window 170. A delivery is then initiated by clicking on the send button 188.

Tracking is accessible from the tracking button 144 on the persistent main tool bar 154. The tracking search function is used to query the CUI database for information about deliveries sent from an account. A sender can therefore find out whether a recipient has received a particular document. The database archive can also be searched for records of past transactions.

Fig. 13 is a view of a CUI tracking search page 222 according to the preferred embodiment of the invention. The secondary navigation from the secondary tool bar 156 includes log 224, search 225, report 226, preferences 228, and help 158. The current function 192, search 225, is identified. The tracking

button on the main tool bar displays a record of all deliveries sent from the account as a delivery log (not shown).

Account managers are permitted to track all deliveries initiated from a group account. Group members are permitted to track only those deliveries initiated personally by the member.

The format of the delivery log is specified in tracking preferences (see Fig. 14). The format chosen applies to both the delivery log and the tracking report (see Figs. 15-17). The preferred embodiment of the invention includes navigation buttons to permit the user to access previous, or subsequent log pages. Information regarding an individual delivery may be displayed on the delivery log, along with an indication of the total number of deliveries logged.

The subject of each listing in the log links to a package detail report (not shown) about the specific delivery. A detail report contains send parameters of each delivery, including a link to the document if not expired, the mimetype, and the message. The detail report also contains the status of the delivery to each recipient, and the charges applied to the transaction. Users can click on log 224 on the secondary tool bar 156 to return to the top level log.

The search function allows users to pinpoint information about, and the status of, a specific delivery or set of deliveries. The user specifies any combination of search criteria to identify the deliveries of interest. If multiple criteria are specified, the search engine performs a logical "AND" search among all the criteria.

In the preferred embodiment of the invention, the search page graphical user interface (GUI) is simplified. A short list 230 of common searchable fields is presented on the Search page. The short list contains five search criteria:

The "To:" field 232 allows a user to search by the intended recipient's full or partial E-mail address of the recipient. Partial e-mail addresses allow the user to search by domain name.

The "From:" field 234 allows an account manager to search according to the originator of the delivery. The account manager selects a member's e-mail address from a pull down menu. For group members and individual account holders, this given user's e-mail is provided and cannot be changed.

The "Subject:" field 236 allows a user to enter keywords which may be found in the subject field of a document.

The "Document:" field 238 allows a user to perform a text search on the name of the document. A user can type in the name of the document, or browse through the list of documents to select a document .

The "Send date:" field 240 allows a user to search for deliveries sent on, before, or after a specific date.

Clicking on the search button 242 initiates the query and returns a report with all deliveries matching the query. Clicking on the reset button 246 clears the form to its default setting.

Clicking on a "More Options..." button 248 at the bottom of the short form brings the user to a page having a second, expanded list (not shown) of searchable fields, including all fields from the short list. In the preferred embodiment, the additional fields in the expanded list include:

The billing code: field allows a user to select from a pre-defined list in a pull down menu.

The "Delivery status:" field allows a user to select from a menu of delivery statuses. Delivery status options include: any, received, not received (includes both failed notification and not picked up), confirmed, not confirmed, pending notification and failed notification. The user may also search document expiration, scheduled notification date, receive date, and message fields.

The search results are presented in a tracking report. The tracking report is presented as a table in a format specified in the tracking preferences dialog. Fig. 14 is a view of a CUI tracking report preferences dialog 250 according to the preferred embodiment of the invention.

The Dialog permits the user to select a document format 252, or to define a new format 254. In the preferred embodiment of the invention, a user can select from two pre-formatted reports, basic format and billing code format. Both summary and detail information reports are available in each format.

The dialog allows the user to specify the number of rows per page 256. Additionally, the user selects whether to show recipient summary information 258, or detail information 260.

Clicking on update 262 saves all changes and returns the user to the report or page from which the user accessed the tracking report. If the user returns to a report, it is displayed with the new preferences settings. The dialog is reset using the reset button 264.

Fig. 15 is a view of a recipient summary tracking report in basic format 266 according to the preferred embodiment of the invention. When search results are displayed, the secondary navigation in the secondary tool bar 156 indicates that the sender is in report mode 226. The elements and behavior of the tracking report are consistent with those of the delivery log.

In the preferred embodiment of the invention, the deliveries are sorted by date and presented in reverse chronological order. However, in alternative embodiments, the deliveries are presented in chronological order, or are sorted, for example, by recipient. The next page of delivery listings is accessed by clicking on the next button 284.

A recipient summary tracking report lists, in the "Recipient(s):" field 270, only the name of the first recipient 268 of a particular delivery, or the first recipient on the mail list to which that delivery was sent. An indication (...) is placed next to the name if there are more names on the list. The number of recipients of the delivery is listed in the "Received:" field 272 and the number notified is listed in the "Notified:" field 274. This information is totaled 276 across all recipients.

For example, the most recent delivery shown in Fig. 15 is the party invite listed in the "Subject:" field 278. The date the party invite was sent was January 22, 1997, as is indicated in the "Sent:" field 280. The tracking report shows that a total of three party invite documents were sent. All three recipients were notified, and received the document. Only the first recipient 268, "jane @isp.com," is listed in the "Recipient(s):" field 270.

Fig. 16 is a view of a recipient detail tracking report in basic format according to the preferred embodiment of the invention. A recipient detail tracking report 282 lists in the "Recipient(s):" field 270 each recipient of each delivery. The "Received:" 272 and "Notified:" 274 fields list the specific dates that each recipient was notified of, and received the delivery. For example, Fig. 16 separately lists the three recipients of the party invite, and their notification and receipt dates.

The recipient detail tracking report also expands every mail list. In the preferred embodiment of the invention, mail lists are only expanded for deliveries that

have been processed. Future scheduled deliveries and deliveries in progress are indicated as such.

Fig. 17 is a view of a recipient detail tracking report in billing code format 286 according to the preferred embodiment of the invention. The billing code format displays the billing code 288 and sorts results by billing code and date.

The CUI account management functions are available from the main tool bar button labeled "Account" 146. Account functions vary according to the type of account and the type of user, such as group account manager, individual account holder, and member account holder. The server software identifies a user's account type and makes the appropriate functions and information available.

All users are able to view administrative account information on record for the respective user's account, including account balance, and can also change their password. Group account managers, however, have extended capabilities. They can edit group members' account information as well as create new accounts. Thus, the secondary navigation of the secondary toolbars displayed to group account managers includes functions such as Information: 302, view members: 304, and add member: 306 (see Fig. 18).

The information page (not shown) displays basic information about the group account that is stored on the dedicated server. Such basic account information includes:

- the name of the account
- type of account
- date it was created
- date it was last accessed
- the number of current members out of the maximum allowed.

Account managers can view and manage the current member list via the Members page (not shown).

Account holder information includes:

- name of the manager
- e-mail address
- company name
- address

The basic account information and the account manager information cannot be edited.

The group account password can be changed from the Information page. The manager enters the existing password and the desired new password, and must confirm the new password. The manager submits the new password by clicking on Update.

In the preferred embodiment, the information page also includes a field which informs the manager when the password was last changed. If the password has never been changed, this field presents the creation date of the account. A link may also be provided to a server manager who is authorized to make changes to accounts.

Managers can view a list of members by clicking on the members text link on the Information page, or by selecting the view members function of the secondary tool bar 156. Fig. 18 is a view of a group account manager account - view members window 288, according to the preferred embodiment of the invention. In one embodiment, managers use a link (not shown) to Preferences

(not shown) where the managers can specify the format, the number of rows per page, and the sorting order of the View Members table.

The view members page displays the name 290 of the group account, and the number 292 of the members displayed out of the total number. The list of members includes the account manager, and is presented in a table which lists the member account names 294, the member names 296, the date created 298, and the date last accessed 300. Clicking on a member's name brings up a "Mailto:" box (not shown), pre-addressed to the member.

Clicking on the account name allows managers to view and edit individual member account information. This information is displayed on a member account information page (not shown) which is similar in format to the group account information page. Basic member account information includes the following (editable information is noted):

- group account
- member account (editable)
- date created
- date last accessed

Member information

- member name (editable)
- e-mail address (editable)

Managers cannot view the member's password, but can change the password on the member account information page by specifying a new password and confirming it. The date of the last password change (not shown) by either manager or member is also displayed. Any changes made to the information

on this page can be submitted by clicking on update (not shown). Reset (not shown) restores the previously stored information.

Member accounts can be completely deleted by clicking on a delete button on the member account information page. Prior to deleting the account, the dedicated server posts a confirmation page notifying the manager of the impending action and requesting confirmation before proceeding. When the member account is updated or deleted, an updated view members window is displayed.

Managers can add members by clicking on the add member link in the secondary tool bar 156. A form (not shown) is displayed prompting the account manager for the information required to create a member account. The form indicates the group account to which the member is added, and the number of the member out of the maximum total members allowed. The information required includes:

- member account name (created by the manger)
- member's name.
- member's e-mail address
- password (and confirm password)

Clicking on add (not shown) creates a new account and returns the manager to an updated view members window. Clicking on reset (not shown) clears the form.

Because individual accounts have no group members aside from the account holder, such individual account holders do not have member information or functions. The secondary tool bar 156 includes only Information (not shown) and help (not shown.) The information displayed from the account information

page is the same as that available from the group account information page, except for the number of current members.

Member account holders also do not have member management functions, and the secondary tool bar includes only information (not shown) and help (not shown). Member account information contains the same basic information as that viewed by managers. However, members are only able to edit e-mail address information.

In the preferred embodiment, members can change their own passwords on the member account information page. They must enter the current password, the new password, and then must confirm the new password. However, in alternative embodiments, members may only be able to change their passwords via the account manager.

The billing button 148 on the main tool bar 154 gives access to billing code mode management and invoice functions. Clicking on the billing button displays a table 320 of defined billing codes. Fig. 19 is a view of a billing codes window 308, according to the preferred embodiment of the invention.

Secondary navigation for billing on the secondary tool bar 156 includes billing codes 310, add codes 312, create invoice 314, view Invoice 316, preferences 318, and help 158.

The table indicates the total number of codes and which ones are currently being viewed 322. In the preferred embodiment of the invention, billing codes are up to 25 characters long and are composed of letters, numbers or characters.

Each billing code 324 has an optional plain English description 326 or name associated with it. In billing preferences (see Fig. 24) the user specifies whether

to sort the billing codes by code or by description, and how many rows to display per page. Preference settings 328 are displayed with the table. Next 330 and Previous (not shown) buttons allow the user to view additional pages of billing codes.

Two levels of billing codes are provided for group accounts. The group manager maintains a list of codes that are accessible by all group members. Group members can select their own subset of codes from the group list for easy access to frequently used codes.

Members cannot edit or create billing codes. They must select codes from the list created by the manager to add to their personal list. Members can specify whether to list group or personal billing codes in billing preferences.

Clicking on a hot-linked billing code allows users to edit or delete the code or its description. Fig. 20 is a view of an edit billing codes window 332, according to the preferred embodiment of the invention. Users can edit a billing code or description from the appropriate fields 338, 340 in the dialog. The information in the fields is cleared using the reset button 342.

Changes are saved by clicking update 334, which returns the user to the billing code table displaying the updated information. Users may also delete 336 codes and descriptions from this dialog. Because group members cannot edit group billing codes, group billing codes are not hot-linked when viewed by a group member.

The add codes function 312 in the secondary navigation is used to add items to a personal billing code list. Fig. 21 is a view of an add billing codes dialog 344 according to the preferred embodiment of the invention.

Managers and individual account holders enter a new code into the "Enter Billing Code:" field 346. Any associated optional description is entered into the "Description:" field 348 in the form provided. The add button 350 is clicked to add the new information to the billing code list. The replace button 352 is clicked to replace information in the billing code list.

Billing codes can also be uploaded 354 from a text file. A browse button 356 is used to locate the appropriate text file for uploading. This text file either replaces or is added to the existing billing code list. When new codes are successfully added, the user is presented with an updated billing code list.

Group members can only add codes from the group billing code list to their personal code list. When group members click on add codes, they are presented with a list box of codes from the group list. They may then select multiple codes from the list box. Once the desired codes are selected, the member clicks on the Add button to add the selected codes to their personal list.

Clicking on the create invoice 314 link allows the user to create an invoice. Fig. 22 is a view of a create invoice window 358, according to the preferred embodiment of the invention. The dialog is a search screen which allows the user to specify which deliveries to bill for the current invoice. Deliveries are billed by billing code or by recipient.

The user selects a billing code or set of billing codes from a list 360 or enters the e-mail address 362 of the recipient. The list contains the billing codes and associated descriptions indicated in billing preferences. Current preferences are displayed 364.

The user also specifies a date range for the invoice's billing period 366. Once the appropriate information is entered, the user clicks create 368 to initiate the query and generate the invoice. Reset 370 clears all entries.

The query result is presented in a pre-formatted basic invoice report window 372 in view Invoice mode, as shown in Fig. 23. The billing code 374 and billing period 376 are displayed, along with the table 378 containing the query results.

The table displays the subject 384 of each delivery, the date sent 390, and the recipient(s) 392. The price 380 and the total 382 of the deliveries are also indicated.

Invoice format is specified in the billing preferences. The subject 384 of each delivery is hot-linked to the package detail report, described above. If the package detail is accessed, the navigation state remains in billing/view invoice. Clicking on view invoice 316 returns the display to the invoice report.

The export button 386 allows users to export the report data as a tab-delimited text file for integration into other existing billing systems. Invoice report preferences 388 (excluding the mark-up rate) are also displayed.

Billing preferences 318 allow users to specify the preferences which affect billing code management and invoice report formats. Fig. 24 is a view of a billing preferences dialog 394 according to the preferred embodiment of the invention.

A pull-down 396 allows group members to choose to use a personal billing code list or a group billing code list maintained by the account manager. All users choose to display lists by billing code 398, or by description 400. This selection affects the display in selection boxes in send options and invoicing.

The selection also affects the presentation of the billing codes display table. If display is by billing code, then the first column is billing code, and the list is sorted by billing code. If display is by description, the first column is description

and the list is sorted by description. The user specifies the number of rows displayed 402 per page.

The user also specifies the rate 404 to charge clients. This rate can be a flat charge 408, or may include a percentage mark-up 406 on top of the costs charged by the user's Internet services provider. The information displayed in the billing preferences dialog can be updated 405 or refreshed 407.

For the invoice report, the user may select a predefined format 410, or define 412 a new format. In the preferred embodiment, the user selects from three predefined formats, the basic invoice, spec invoice, and billing code invoice formats. The basic invoice format has previously been shown in Fig. 23.

Fig. 25 is a view of an Invoice report in spec invoice format according to the preferred embodiment of the invention. The spec invoice 414 displays the total number 416 of recipients for each delivery as well as the size 418 of the document. This information is sorted chronologically.

Fig. 26 is a view of an invoice report in billing code invoice format according to the preferred embodiment of the invention. The billing code invoice format 420 is sorted by billing code 422, as well as by date.

The CUI allows publishers and other users to create and manage distribution lists. Fig. 27 is a view of a mail list page 424 according to the preferred embodiment of the invention. Mail list functions are accessible from the main tool bar 154. Secondary navigation includes mail list 426, create list 428, preferences 530 and help 158.

There are two levels of mail lists for group accounts, i.e. group and personal. Group lists are managed by the account manager and are accessible to all group members. A group member can define a personal list accessible only by

that group member. Each member can specify which set of lists to use in their mail list preferences.

Clicking on the mail list button 150 on the main tool bar 154 displays a table 432 listing existing mail lists 434. The table also presents the total number 436 of recipients on each mail list and the date 438 the mail list was most recently modified. The preferences settings 440 are also displayed.

In mail list preferences (not shown), the user specifies whether to sort the items by the name of the mail list or by date. Current preferences are displayed in the mail lists dialog. Next and previous buttons (not shown) may be provided to navigate between pages of mail lists.

Clicking on the hot-linked name 442 of a mail list brings up a mail list detail for the selected mail list. Fig. 28 is a view of a mail list detail window 444, according to the preferred embodiment of the invention.

The mail list detail page displays general information about an existing mail list and allows the user to view and manage mail list addresses. Group members cannot manipulate group mail lists. Therefore, the mail list detail of group lists does not display fields for editing. Group members can, however, edit personal mail lists.

Account Managers can manipulate group mail lists. The detail 444 presented to account managers displays the name 446 of the mail list in an editable form. To rename the list, the user changes the name in the form and clicks on the update button 448. Users may also delete 450 the entire mail list or add addresses 452 by clicking on the appropriate button. The total recipients 454 and date last modified 456 are also displayed.

The detail also displays the mail list addresses 458. In the preferred embodiment of the invention, the first page of the complete address list is displayed in accordance with the number of rows per page specified in the mail list preferences. The detail indicates which addresses out of the total are displayed. Next and previous links (not shown) may be provided to navigate between multiple pages of addresses.

The user can also view a select set of addresses by specifying a query in the field 460 provided. For example, an e-mail address or a portion of an address such as a domain name can be specified. Clicking on the view button 462 then displays a table 464 of matching addresses 458. The table indicates which addresses 466 out of the total matching set of addresses are displayed.

The user edits or deletes individual addresses in the table by clicking on the appropriate address. An edit page (not shown) with update and delete buttons is then displayed. When the address is updated or deleted, users are returned to an updated mail list detail page.

From the detail page, users can also delete multiple addresses at a time. Clicking on the "delete items on page" button 468 deletes all the addresses in the table. Clicking on "delete all matching items" 470 deletes all items which matched the query, whether or not the addresses are visible on the current page. A warning message asking the user to confirm the action is displayed before the dedicated server actually deletes the addresses. Once the addresses are deleted, the detail page is immediately updated and presented to the user.

Clicking on the add addresses button 452 in the mail list detail 444 displays the add addresses page. Fig. 29 is a view of an Add Addresses window 472 according to the preferred embodiment of the invention. The name of the

current mail list 474 is displayed at the top. The name is also linked to the mail list detail page.

The user can add additional addresses by manual entry 476, by uploading them from a file. The user can enter a file name 478, or use the browse button 480 to search all files. Names may also be obtained from an existing mail list 482 and merged with the current mail list. The additional addresses are added 484 to the current address list or replace 486 the current list. After the names are submitted, the users are returned to an updated member detail page with a line at the top confirming the addition or replacement that just occurred.

The user can create a new mail list by clicking on the create list link 428 from the secondary navigation. In the preferred embodiment of the invention, the create mail list page (not shown) is similar to the add addresses page. However, in the create mail list page, the user is prompted for the name of the mail list.

The user can manually enter addresses in the provided text box. Alternatively, the user can upload addresses from a file or copy addresses from an existing mail list. However, because the user is creating a new list, there is no option provided to replace an existing list. Clicking add creates a mail list with the specified names and addresses. The user is presented with an updated mail list report, with the new list information included.

The invention also provides security for restricting access to the system to an authorized user. The types of security supported by the invention include authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication. This security is provided by a security framework that includes at least one security module, in at least one of the send client application, the receive client application , and the GUI.

Fig. 30 is a flow chart of the method for delivering a document over an electronic network, according to the invention. The sending computer establishes a session (500), for example, over the Internet. The sending computer then delivers the document to a dedicated server (505) over this electronic network, using a send client application.

The send client application preferably includes modules for sending documents, listing document activities, tracking documents, specifying and storing document parameters, and for providing security features (510). Any or all of these modules may be accessed during a particular session.

The dedicated server stores the document (515) and forwards an electronic notification message to the receiving device (530). The dedicated server is managed via a configuration user interface (520). The configuration user interface preferably includes modules for sending documents, tracking documents, accounting, billing, generating mail lists, as well as a security feature module (525).

In response to the notification message, the receiving device downloads the document (535) from the dedicated server using a receive client application. The receive client application preferably includes modules for downloading, viewing, and manipulating the document, as well as for providing security (540).

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention. The invention is readily constructed and configured by one skilled in the art, using well-known programming techniques and equipment.

For example, the placement and contents of the toolbars and menus in the desktop displays described herein is for exemplary purposes only. Furthermore, the functions of the invention may be accessed by alternate means, including icons, and keyboard text entries.

In one embodiment of the invention, the notification message regarding a document delivery is received by a notification receiving device. The document can then be retrieved by a receiving device that is either included in the notification receiving device, or is separate therefrom. For example, the notification message can be received on a pager or personal digital assistant, and the document received on a personal computer using a Web browser.

The sender driven certificate enrollment system (SDCE) 42 enables corporations, publishers and individuals to securely distribute documents electronically, by allowing the sender to initiate and control the implementation of digital certificate enrollment to one or more recipient clients.

Fig. 31 shows a basic certificate enrollment system 1342a implemented between a sending computer 1352 and a receiving computer 1370 across a network 1344, which may include an internet. Fig. 32 shows a certificate enrollment system 1342b implemented between a sending computer 1352, a SDCE server 1358 and a receiving computer 1370. Fig. 33 shows a certificate enrollment system 1342c implemented between a sending computer 1352, a SDCE server 1358, a database server 1362 and a receiving computer 1370. Fig. 34 shows a certificate enrollment system 1342d implemented between a sending computer 1352, a SDCE server 1358, a database server 1362, a certificate server 1388 and a receiving computer 1370.

The sender driven certificate enrollment system 1342 enables the sender 1352 of a document 1312 to initiate the generation of a digital certificate 1345, (see Fig. 35) on behalf of an intended recipient 1370 of a document. A document

1312 can mean a specific computer file or more generally any discrete collection of data. The sender driven certificate enrollment system 1342 simplifies the associated complexity of generating a digital certificate for an intended recipient 1370 of a document, and transfers the primary burden of certificate generation from the recipient 1370 (which many systems support today) to the sender 1352. Fig. 35 shows a digital certificate 1345, which denotes a key pair comprising a public 1332 and private key 1340, where the public key 1332 is associated with a specific entity, such as an intended recipient 1370, and is published.

One of the main problems associated with secure document delivery stems from the challenge of encrypting a document 1312 with the public key 1332 of the intended recipient 1370. In particular, the intended recipient 1370 of a document may not have a digital certificate 1345. In the absence of a digital certificate 1345 of the recipient 1370 which is accessible by the sender 1352, the sender 1352 of a document 1312 cannot encrypt the document 1312 with the recipient's public key 1332, and hence cannot be assured that the document 1312 can be protected from unsolicited access. The sender driven certificate enrollment system 1342 allows the sender 1352 of a document 1312 to initiate the process of dynamically generating a digital certificate 1345 for the intended recipient 1370, thereby imposing minimum requirements for the intended recipient 1370.

The sender driven certificate enrollment system 1342 transfers the burden of certificate generation from the recipient 1370 of a given document 1312 to the sender 1352. The sender driven certificate enrollment system 1342 exploits the fact that, in the context of document delivery, often the sender 1352 of a document 1312 has unique and specific information regarding the intended recipient 1370. Suppose, for example, an attorney sends a document to a client 1370. The attorney 1352 likely has a record associated with the client 1370 which contains specific information, such as the client's e-mail address,

physical address, telephone number. The client record may also contain confidential information, such as the client's social security number, drivers license number, or even credit information.

Typically, it is this type of confidential information which is utilized to authenticate a given individual or entity 1370, and hence generate a digital certificate 1345. Highly confidential and specific information yields a high level of authentication, and hence a secure digital certificate.

Therefore, the sender driven enrollment system 1342 exploits the fact that the sender 1352 often knows significant and confidential information regarding an intended recipient 1370 of a document 1312. The use of this confidential information by the sender 1352 to generate a digital certificate 1345 minimizes the burden imposed on the recipient 1370 to confirm their identity. The digital certificate 1345 is then utilized by the sender 1352 to securely send the document 1312 to the intended recipient 1370.

System Implementation. In the example above, a sender attorney 1352 wishes to send a confidential document to an intended recipient client 1370. For a client 1370 that does not currently have a digital certificate 1345 accessible to the attorney 1352, the attorney 1352 can invoke the sender driven enrollment system 1342 to generate a digital certificate 1345 for the client 1370.

First, the sender driven enrollment system 1342 checks or queries a database 1346 to determine if a digital certificate 1345 exists for the recipient client 1370. If not, the sender driven enrollment system 1342 conducts a database query to pull up a record for the client 1370, which typically includes client specific and confidential information.

The sender driven certificate enrollment system 1342 then generates a certificate digest 1347, as shown in Fig. 36. This certificate digest 1347

contains most of the information necessary to generate a digital certificate 1345 for the client 1370, including the client specific data 1348, and the type of certificate to generate 1349 (e.g. an X.509 certificate). In a preferred embodiment, the certificate digest 1347 is forwarded to a secure SDCE server 1358. The SDCE server 1358 then "contacts" the client 1370, seeking independent confirmation of the confidential information 1348. For example, in a preferred embodiment of the invention, the SDCE server 1358 forwards an e-mail message to the client 1370 with a unique, dynamically generated URL (uniform resource locator). The client 1370 can then "click" or access this URL through a standard web browser. Accessing the URL begins a direct interaction, or SDCE conversation 1368, between the client 1370 and the SDCE server 1358.

The client 1370 is typically asked to input one or more pieces of confidential information 1348 to the SDCE server 1358. In a preferred embodiment, the conversation takes place over a secure socket layer (SSL) channel between client 1370 and the SDCE server 1358, and utilizes HTML forms.

The SDCE server 1358 then attest whether the client 1370 is correct, by comparing input information to the stored client information 1348 within the stored certificate digest 1347. On a match, the SDCE server 1358 forwards the certificate digest 1347 over a secure channel to the recipient client's desktop 1372, and also distributes software to the recipient client 1370, which uses the certificate digest 1347 to generate a key pair 1332, 1340 on the recipient system. In the preferred embodiment of the invention, this software is simply a Java applet, transparently forwarded to the recipient 1370 through the browser. The generated private key 1332 is stored on the recipient system 1370, preferably using the PKCS12 format. The public key 1332 is forwarded back to the SDCE server 1358, which typically registers both the public and client information as the digital certificate 1345 on a certificate server 1388, such as

an LDAP or an Entrust certificate management server (of Entrust, Inc., Ottawa, Canada).

The sender (e.g. the attorney) 1352, can now access the stored public key 1332 for the intended recipient client 1370, encrypt the document 1312 intended for the recipient client 1370 with the public key 1332, and then send the encrypted document 1336 to the client 1370. The client 1370, in turn, decrypts 1338 the encrypted document 1336 with [the public key and] the corresponding private key 1340, which is now resident on the private recipient system 1370.

Fig. 37 shows the first stage 1350 of the sender driven certificate enrollment system 1342. A sender 1352 initiates the generation of a certificate for a recipient 1370 at step 1356, by contacting an SDCE server 1358 and forwarding basic information to identify the recipient 1370, such as an e-mail address.

The SDCE server 1358 then queries a database 1346, at step 1360, for confidential information 1348 specific to an intended recipient 1370, such as a social security or personal address. The database 1346 may reside at any of a number of locations, such as within a separate database server 1362, or within the SDCE server 1358.

If usable confidential information 1348 exists for an intended recipient 1370, it is transferred, at step 1364, as a data record to the SDCE server 1358. The SDCE server 1358 then uses the data record to generate a certificate digest 1347, at step 1365, which is later used to attest the recipient 1370 and to generate a digital certificate 1345.

Fig. 38 shows the second stage 1366 of the sender driven certificate enrollment system 1342, referred to as an attestation conversation. The SDCE server 1358 takes the certificate digest 1347 and initiates a direct interaction, at step 1368,

with the intended recipient 1370 of a document 1312. This direct interaction 1368 solicits client specific data 1348 from the intended recipient 1370.

In a preferred embodiment of the invention, the SDCE server 1358 sends an e-mail message with a dynamically generated Uniform Resource Locator (URL). The recipient 1370, by clicking on the generated URL, invokes a direct interaction 1368 with the SDCE server 1358. At this point, the SDCE server 1358 presents HTML forms soliciting specific information from the recipient 1370.

The HTML forms and requested private information 1348 may vary, depending on the level of security desired for the document 1312 to be sent to the recipient 1370. For example, for a document that does not require a high level of security, the forms might simply request a confirm button. For a document that requires a higher level of security, the form might ask the intended recipient 1370 to submit specific private information 1348, such as a personal address, a social security number, and employee number or personal identification number (PIN). In a preferred embodiment of the invention, this interaction between the SDCE server 1358 and the recipient 1370 takes place over a secure channel using SSL.

Using the forwarded private information 1348, through step 1374, the SDCE server then attests the recipient 1370 by comparing the forwarded data 1348 to the certificate digest 1347 for the intended recipient 1370. If the forwarded information 1374 and the appropriate stored information 1348 in the certificate digest 1347 match, the recipient 1370 is authenticated, at step 1375, and the process continues to the next stage. If the forwarded 1374 information and the appropriate stored information 1348 in the certificate digest 1347 do not match, the sender 1352 is notified that no digital certificate 1345 has been generated (Fig. 41).

Fig. 39 shows the third stage 1376 of the sender driven certificate enrollment system 1342, referred to as public/private key pair generation. Assuming that the private information 1374 solicited over the attestation conversation stage 1366 matches the certificate digest 1347 at the SDCE Server 1358, the SDCE server 1358 then forwards software and the certificate digest 1347 to the recipient system 1370, at step 1378. The forwarded software utilizes the certificate digest 1347, and information local to the recipient computer 1370, to generate a digital certificate 1345, comprising private/public key pair 1332, 1340. The key pair 1332, 1340 is sent to and stored locally on the sender system 1352. In a preferred embodiment, the public/private key pair 1332, 1340 is stored in a PKCS12 format. The public key 1332 and a reference to the certificate digest 1347 for the recipient 1370 is then forwarded from the receiver 1370 to the SDCE server 1358.

Fig. 40 shows the fourth stage 1384 of the sender driven certificate enrollment system 1342, referred to as forwarding and registration of the receiver public key 1332. At this stage in the process, the public key 1332 for the intended recipient 1370 has been forwarded from the recipient system 1370 to the SDCE server 1358. The SDCE server 1358 forwards the public key 1332 and the certificate digest 1347, combined as a digital certificate 1345, to a certificate server 1388, at step 1386. In a preferred embodiment, the certificate server 1388 is an LDAP (Lightweight Directory Access Protocol) server. The SDCE server 1358 then sends a notification back to the sender 1352, at step 1390, that indicates that the document 1312 can now be encrypted 1334 with the public key 1332 of the recipient 1370, as shown in Fig. 3. The encrypted document 1336 is then delivered to the recipient 1370, typically across a network or internet architecture 1344. The recipient 1370 then uses their own private key 1340 to decrypt the information, as shown in Fig. 4.

Implementation. This section provides an overview of the components to construct a sender driven certificate enrollment system 1342. Some of the

components, such as the certificate server 1388 do not require any customization or development. Fig. 41 is a basic flow chart that describes the flow of control for the system.

Sender Desktop Client Software. On the desktop 1354 of the sender computer 1352, the sender driven certificate enrollment system 1342 includes software which communicates with the SDCE server 1358 and the certificate server 1388 to query the public key 1332 associated with the recipient 1370. The recipient software component, upon retrieval of the public key 1332 for the recipient 1370, typically encrypts a document 1312 with the public key 1332 and then forwards the document to the SDCE server 1358 for subsequent delivery to the recipient 1370.

SDCE Server Software. The SDCE Server software, in a preferred embodiment of the invention, includes a HTTP Web Server with a customized filter to intercept and redirect all HTTP requests, a e-mail server to forward notifications on to an intended recipient 1370, and the basic software and logic to query a database server, to generate a certificate digest 1347 (as described above), and to interact with all other components of the system.

The Web server is a primary interface between the SDCE server 1358 and the intended recipient 1370 of a document 1312, in which the SDCE server 1358 assists in the construction of a digital certificate 1345.

In a preferred embodiment of the invention, the SDCE server software initiates an attestation conversation 1366 (Fig. 38) with the intended recipient 1370, by dynamically generating a private URL. The private URL contains a key to uniquely identify the recipient 1370, and then forwards this "key" to the recipient over a standard e-mail notification. When the recipient 1370 accesses this "key" (which in fact is a private URL), the SDCE server 1358 associates the key with a given certificate digest 1347, and then through the Web interface, conducts the

attestation conversation 1366, to verify that the given recipient 1370 matches the parameters of the certificate digest 1347.

Recipient Client Software. The sender driven certificate enrollment system 1342 creates a public/private key pair from a certificate digest 1347, which is forwarded from the SDCE server 1358 to the recipient system 1370. Client software on the recipient computer takes the certificate digest 1347, constructs the public/private key pair 1332, 1340 on the recipient desktop 1372, stores these keys 1332, 1340 on the recipient system 1370, and then forwards the public key 1332 to the SDCE server 1358.

In a preferred embodiment, the recipient client software is a Java applet, which is transparently and dynamically downloaded via a web browser, in which the recipient simply accesses an URL, as described above.

Certificate Server. The invention makes use of basic digital certificate management. The certificate server 1388 includes query ability, which determines if a digital certificate exists for a recipient given a specific user profile (*e.g.* an e-mail address and identifier). The certificate server 1388 also includes update ability, which allows a programmatic interface to add a new certificate to the server's database. In preferred embodiments, LDAP, X.500, or proprietary certificate servers such as a Entrust server can be used as certificate servers 1388.

Database Server. In a preferred embodiment of the invention, the SDCE server 1358 queries a database 1346 containing recipient information to construct a certificate digest 1347. In a basic embodiment, the sender's desktop 1354 can query an internal database 1346, or the sender's desktop 1354 can simply load information directly from the desktop 1354. The preferred database query provided by a SDCE server 1358 supports more scalability and extensibility.

In addition to the basic design for the invention, there remains situations wherein no recipient data 1348 exists which is readily accessible from the senders system 1352, either directly from the desktop 1354 or via a database query. In this case, the sender driven enrollment system 1342 still retains value. While the certificate digest 1347 contains limited information 1348, the level of attestation is also limited. However, basic attestation can still take place, and the system 1342 still simplifies the process of generating a basic digital certificate 1345 for the recipient 1370. In this case, the system behaves exactly as designed, with the exception being a more simplistic conversation 1366 and certificate digest 1347.

Fig. 41 is flow chart 1302 that describes the basic decision tree behind the sender driven certificate enrollment system 1342.

At step 102, the sender 1352 queries the certificate server 1388 for the public key 1332 of an intended recipient 1370 for a document 1312. If the public key 1332 exists, the document 1312 is encrypted with the public key 1332, and is sent to the recipient 1370, at step 104. If the public key 1332 doesn't exist, the sender queries the SDCE Server 1358 for a certificate digest 1347 for the intended recipient 1370, at step 1356.

The SDCE server 1358 then queries the database 1346 for information 1348 regarding the intended recipient 1370, at step 1360. If the information exists and is already stored in the database 1346, the SDCE server 1358 generates a rich certificate digest for the client 1370, at step 1365. If no information 1348 exists and is stored in the database 1346, the SDCE server 1358 generates a simplified certificate digest 1347, at step 1364.

At step 1368, the SDCE server 1358 initiates an attestation conversation 1366 with the recipient 1370. If there is no match to the information 1348, the SDCE server 1358 notifies the sender 1352, at step 106, and there is no generation of

a key pair 1332, 1340. If there is a match, a private/public key pair 1332, 1340 for the recipient 1370 is generated on the recipient system 1370, at step 1380. The key pair is then forwarded to the SDCE server 1358, at step 1382. At step 1388, the SDCE server registers the certificate for the intended recipient 1370 with a certificate server 1388. At step 1390, the SDCE server notifies the sender 1352 of the digital certificate 1345. The sender 1352 can then encrypt the document 1312 with the generated public key 1332 of the intended recipient 1370, as shown in Fig. 3. When the encrypted document 1336 is sent to the recipient 1370, typically over a network 1344, the recipient 1370 can decrypt the encrypted document 1336, using the stored private key 1340, as shown in Fig. 4.

Although the sender driven certificate enrollment system and its methods of use are described herein in connection with use in the Internet, the invention may be applied to any of a wide variety of networks, including internets, intranets, LANs and WANs, or any combination thereof, as desired. As well, the invention may be applied to a wide variety of computer platforms, servers, communication protocols, cryptography protocols, or any combination thereof, as desired.

Although the present invention has been described in detail with reference to a particular preferred embodiment, persons possessing ordinary skill in the art to which this invention pertains will appreciate that various modifications and enhancements may be made without departing from the spirit and scope of the claims that follow. Accordingly, the invention should only be limited by the Claims included below.

CLAIMS

1. An apparatus management and delivery system comprising:

a send client application for delivering at least one document as a single package from a sending computer over an electronic network during a session;

a dedicated server for storing said at least one document from the sending computer and for forwarding an electronic message to a receiving device; and

a receive client application on said receiving device for downloading, viewing, and/or manipulating said at least one stored document from the dedicated server in response to the electronic message.

2. The apparatus of Claim 1, wherein said send client application further comprises a package window for specifying parameters of the document delivery.

3. The apparatus of Claim 1, wherein said send client application further comprises a storage module for configurably storing said specified document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

4. The apparatus of Claim 1, wherein said send client application further comprises a module for accessing an address book from a supported application on said sending computer, wherein said document delivery is initiated using the contents of said address book.

5. The apparatus of Claim 1, wherein said document is delivered by selecting and dragging said document onto one of an application window, a package window, an icon representing said send client application, or an icon for accessing said stored document delivery parameters.

6. The apparatus of Claim 14, wherein said Configuration User Interface comprises:

a sending module for sending said document;

a tracking module for tracking said document;

an account CUI for accessing information associated with a document delivery account;

a billing module for managing billings for said document delivery; and

a mail list module for creating and managing mail distribution lists.

7. The apparatus of Claim 1, further comprising a security framework for restricting access to said apparatus and/or to said document, said security framework having at least one security module in at least one of said send client application, said receive client application, and a configuration user interface.

8. The apparatus of Claim 19, wherein said security framework supports at least one of authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication.

9. A document management and delivery apparatus for an electronic network, comprising:

a dedicated server for electronically notifying a notification receiving device on an electronic network of at least one document stored on said dedicated server;

a receiving device on said electronic network for receiving said at least one document in response to said notification;

wherein said receiving device uses a receive client application to download said document from said dedicated server.

10. The apparatus of Claim 9, wherein said receiving device includes said notification receiving device.

11. The apparatus of Claim 9, further comprising an HTML interface on a computer desktop for managing said dedicated server via a Web browser.

12. The apparatus of Claim 9, further comprising a send client application for delivering said at least one document as a single package from said desktop of a sending computer over said electronic network during a session.

13. The apparatus of Claim 12, said send client application comprising:

an application window for displaying a send client application interface, said application window comprising a tool bar for accessing main functions of said send client application, a package manager for listing all document activities initiated during a send client application session, and a menu listing operational commands for said send client application;

a package window for specifying the parameters of said document delivery; and

a storage module for configurably storing said document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

14. The apparatus of Claim 24, further comprising a security framework for restricting access to said apparatus and/or said document.

15. A method for document management and delivery on an electronic network, comprising the steps of:

delivering at least one document as a single package from a sending computer to a dedicated server over an electronic network during a session using a send client application;

storing said at least one document from said sending computer on said dedicated server;

forwarding an electronic message to a receiving device from said dedicated server ; and

downloading said at least one stored document from said dedicated server using a receive client application on said receiving device, in response to the electronic message.

16. The method of Claim 15, further comprising the step of:

said sending computer desktop displaying an application window with a send client application interface having a tool bar for accessing main functions of said send client application, a package manager for listing all document activities initiated during said session, and a menu listing operational commands for said send client application.

17. The method of Claim 40, comprising the step of:

configurably storing, in a storage module, said specified document delivery parameters, wherein said document delivery is initiated using said stored document delivery parameters.

18. The method of Claim 15, further comprising the step of:

providing a security framework for restricting access to said system, said security framework supporting at least one of authentication layers, secure socket layers, password protection, private key encryption, public key encryption, and certificate authentication.

19. The method of Claim 15, further comprising the step of:

initiating said document delivery from the contents of an address book of a supported application on said sending computer.

20. The method of Claim 15, comprising the step of:

displaying a Configuration User Interface application window for managing said dedicated server on a computer desktop, said configuration user interface application window having a main tool bar for accessing main functions of said configuration user interface, a secondary tool bar for accessing

functions within said main functions, a workspace for displaying an interactive interface to an accessed function, and a menu listing operational commands for said configuration user interface.

21. An apparatus for generating a digital certificate for a recipient by a sender, comprising:

a sending computer for use by said sender;

a receiving computer for use by said recipient;

a database for storing recipient information;

means for querying said database by said sender for said stored recipient information;

means for gathering private recipient information from said recipient;

means for comparing said gathered private recipient information and said stored recipient information;

means for controllably generating a digital certificate comprising a public key and a private key at said receiving computer;

means for storing said digital certificate; and

means for transferring said public key to said sending computer.

22. The apparatus of Claim 21, further comprising:

a server interposed between said sending computer and said receiving computer.

23. The apparatus of Claim 22, wherein said database for storing recipient information is located on said server.

24. The apparatus of Claim 22, wherein said means for querying said database by said sender for said stored recipient information is located on said server.

25. The apparatus of Claim 22, wherein said means for gathering private recipient information from said recipient is located on said server.

26. The apparatus of Claim 22, wherein said means for comparing said gathered private recipient information and said stored recipient information is located on said server.

27. The apparatus of Claim 22, wherein said means for storing said digital certificate is located on said server.

28. The apparatus of Claim 21, further comprising:

a certificate digest comprising said stored recipient information and sender selectable options for said digital certificate.

29. A method for generating a digital certificate for a recipient by a sender, comprising the steps of:

querying a database for stored recipient information;

gathering information from said recipient;

comparing said gathered information with said queried, stored recipient information;

selectively transferring software to said recipient based upon said comparison; and

selectively generating said digital certificate at said recipient with said software, said digital certificate comprising a public key and a private key.

30. The method of Claim 29, further comprising the step of:

transferring a copy of said digital certificate to said sender.

31. The method of Claim 29, further comprising the step of:

transferring a copy of said public key to said sender.

32. The method of Claim 29, wherein said database for storing recipient information is located on a server.

33. The method of Claim 29, wherein said step of querying said database is performed by a server.

34. The method of Claim 29, wherein said step of gathering information from said recipient is performed by a server.

35. The method of Claim 29, wherein said step of comparing said gathered information with said queried, stored recipient information is performed by a server.

36. The method of Claim 29, further comprising the step of:

generating a certificate digest comprising said stored recipient information and sender selectable options for said digital certificate.

37. An apparatus for controllably generating a digital certificate for a recipient by a sender, comprising:

a sending computer for use by said sender;

a receiving computer for use by said recipient;

a database for storing recipient information;

means for gathering information from said recipient; and

means for controllably generating a digital certificate for said recipient if said gathered information and said stored recipient information match.

38. The apparatus of Claim 37, further comprising:

a server interposed between said sending computer and said receiving computer.

39. The apparatus of Claim 38, wherein said database for storing recipient information is located on said server.

40. The apparatus of Claim 38, wherein said means for gathering information from said recipient is located on said server.

41. The apparatus of Claim 38, wherein said means for controllably generating a digital certificate is located on said server.

42. The apparatus of Claim 38, wherein said means for controllably generating a digital certificate includes software that is downloadable from said server to said receiving computer.

43. The apparatus of Claim 38, wherein said server includes means for storing said digital certificate.

44. The apparatus of Claim 37, further comprising:

a certificate digest comprising said stored recipient information and sender selectable options for said digital certificate.

Fig. 1
(PRIOR ART)

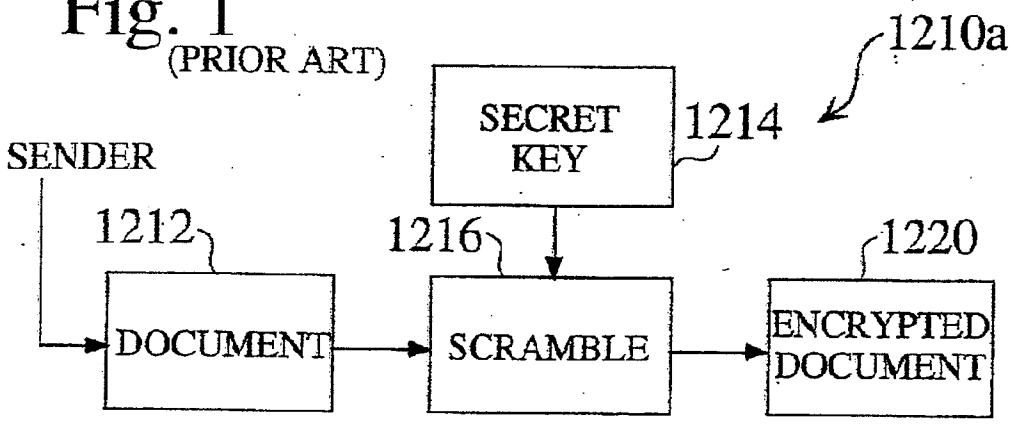


Fig. 2
(PRIOR ART)

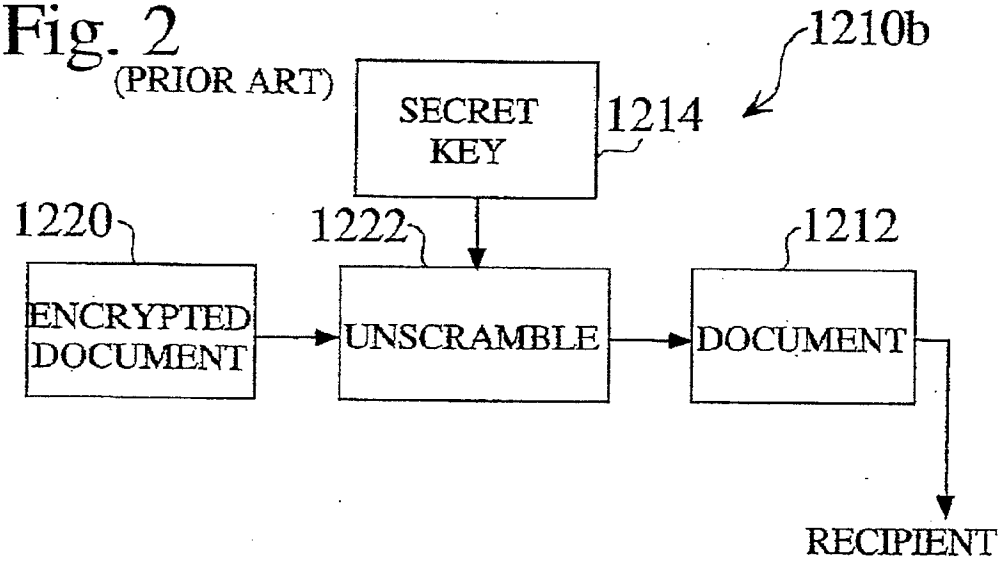


Fig. 3

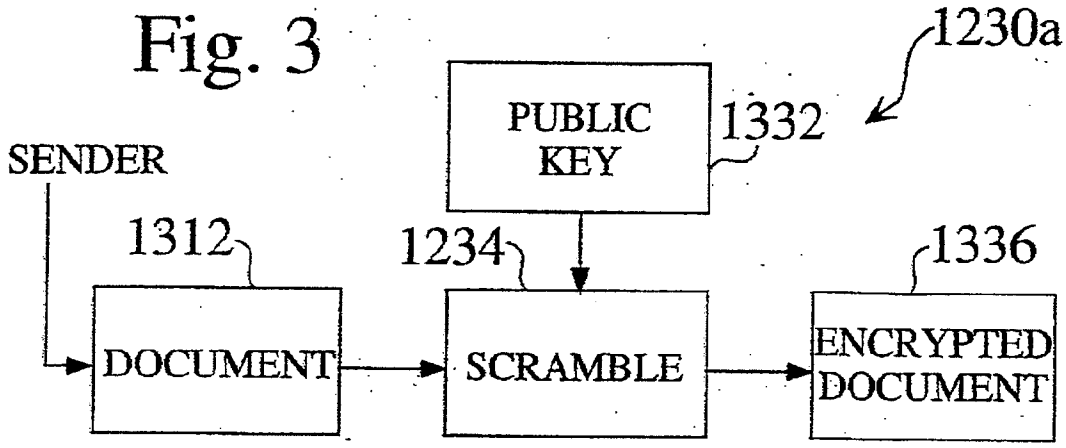
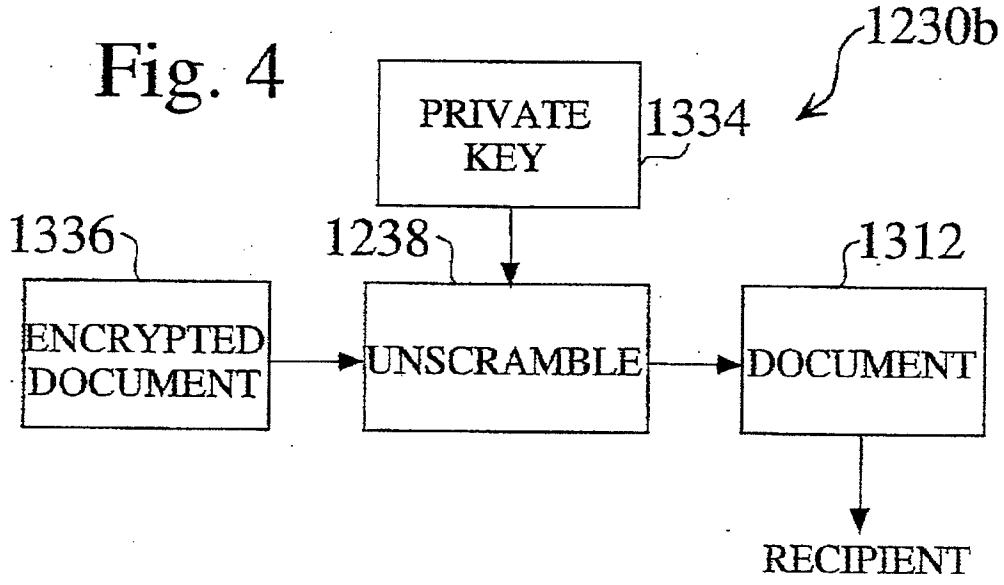

1230a
PUBLIC KEY
1332
SENDER
1312
1234
1336
DOCUMENT
SCRAMBLE
ENCRYPTED DOCUMENT

Fig. 4


1230b
PRIVATE KEY
1334
1336
1238
1312
ENCRYPTED DOCUMENT
UNSCRAMBLE
DOCUMENT
RECIPIENT

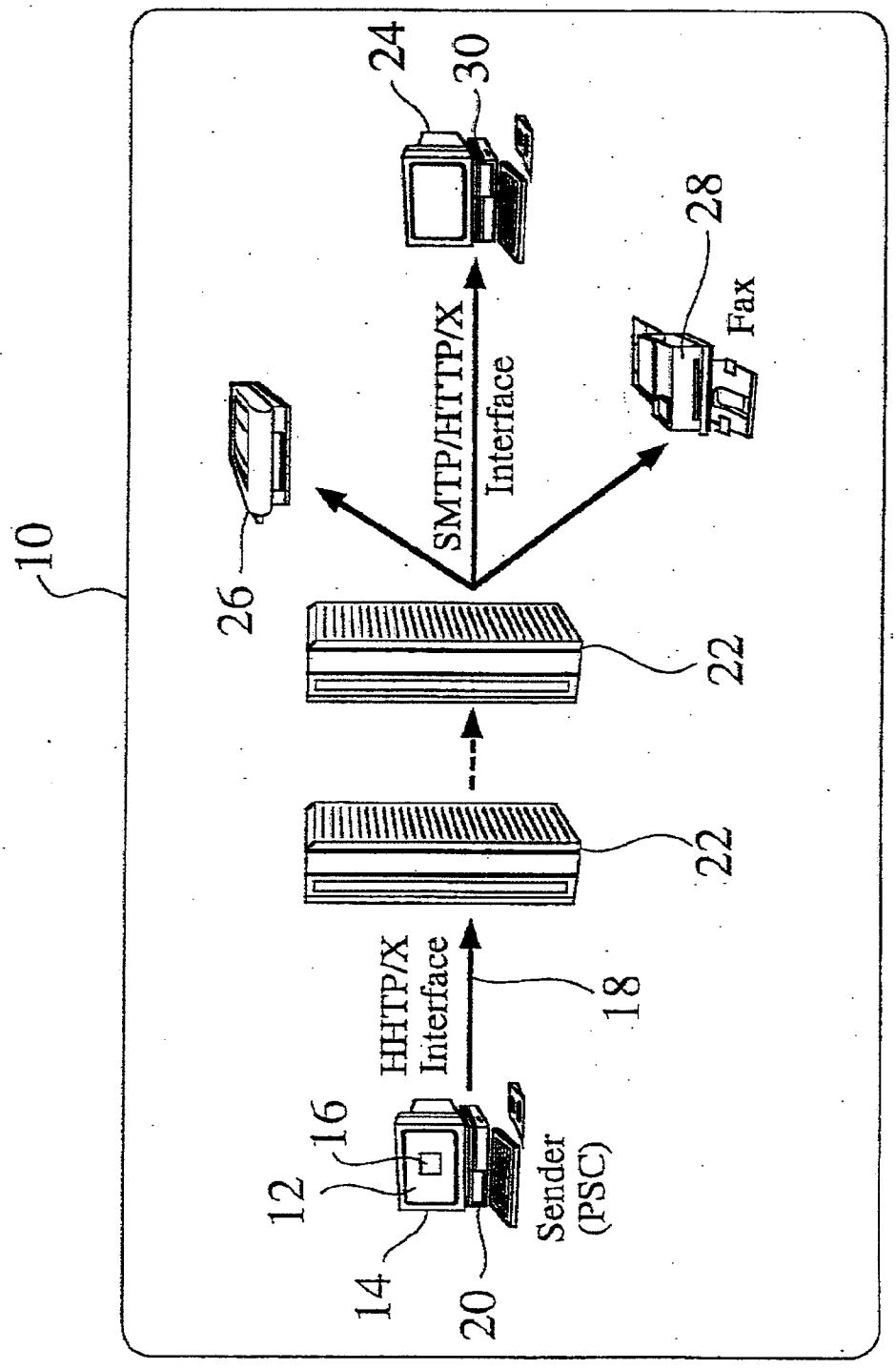

10
12
16
14
20
Sender
(PSC)
HHTP/X
Interface
18
22
22
26
SMTP/HTTP/X
Interface
24
30
28
Fax

Fig. 5

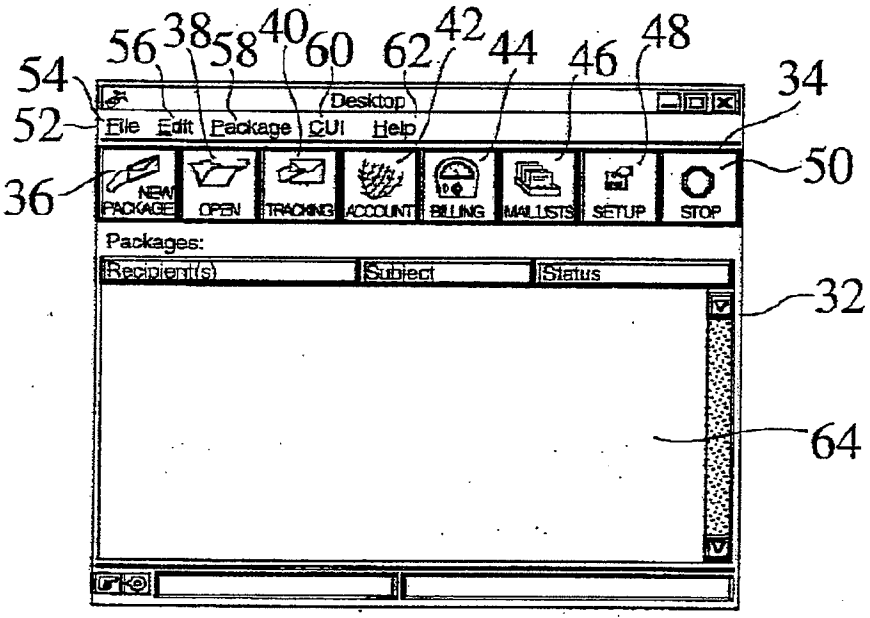

54
56
38
58
40
60
62
42
44
46
48
34
52
File
Edit
Package
CUI
Help
Desktop
36
NEW PACKAGE
OPEN
TRACKING
ACCOUNT
BILLING
MAILLISTS
SETUP
STOP
50
Packages:
Recipient(s)
Subject
Status
32
64

Fig. 6

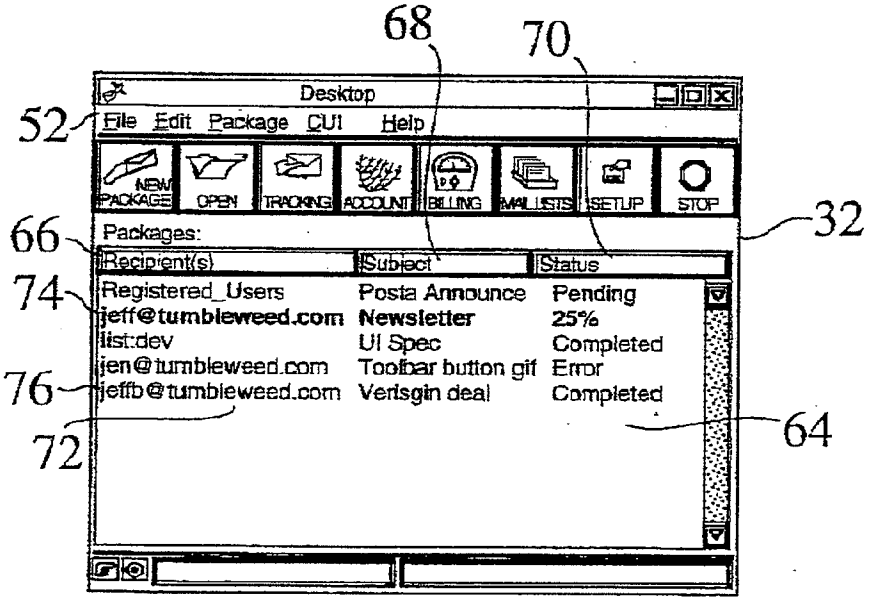

68
70
Desktop
52
File Edit Package CUI Help
NEW PACKAGE
OPEN
TRACKING
ACCOUNT
BILLING
MAILLISTS
SETUP
STOP
32
Packages:
66
Recipient(s)
Subject
Status
74
Registered_Users Posta Announce Pending
jeff@tumbleweed.com Newsletter 25%
list:dev UI Spec Completed
jen@tumbleweed.com Toolbar button gif Error
76
jeffb@tumbleweed.com Verisgin deal Completed
72
64

Fig. 7

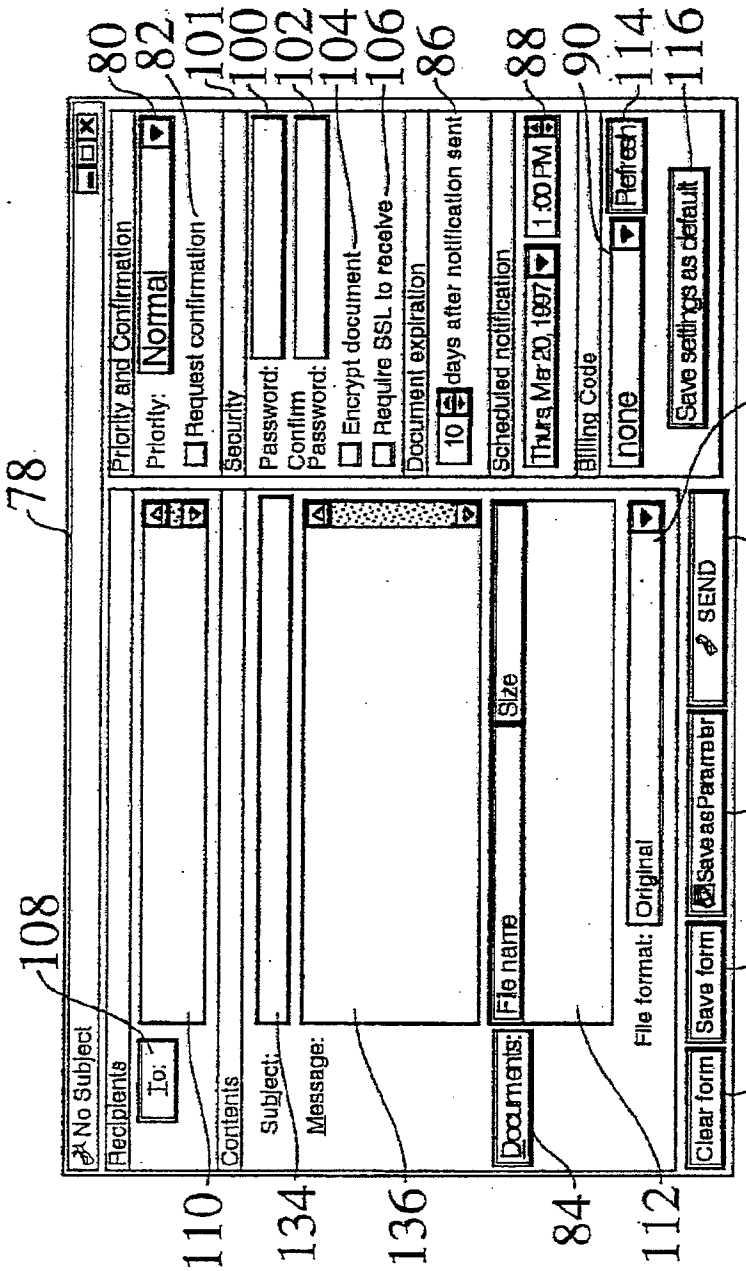

No Subject
Recipients
To:
Contents
Subject:
Message:
Documents:
File name
Size
File format:
Original
Priority and Confirmation
Priority:
Normal
Request confirmation
Security
Password:
Confirm Password:
Encrypt document
Require SSL to receive
Document expiration
10
days after notification sent
Scheduled notification
Thurs, Mar 20, 1997
1:00 PM
Billing Code
none
Refresh
Save settings as default
Clear form
Save form
Save as Parameter
SEND
78
80
82
101
100
102
104
106
86
88
90
114
116
108
110
134
136
84
112
92
94
96
98
138

Fig. 8

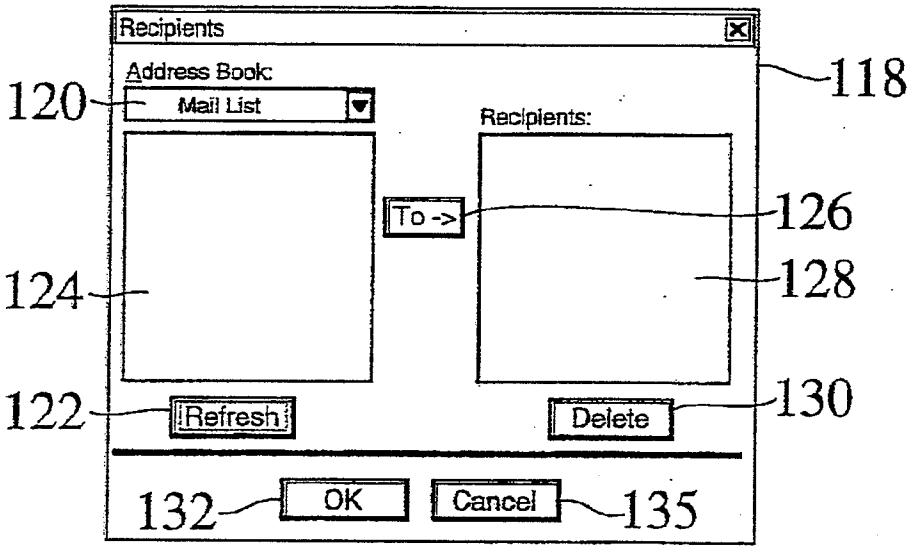

Recipients
Address Book:
Mail List
Recipients:
To ->
Refresh
Delete
OK
Cancel
118
120
124
126
128
122
130
132
135

Fig. 9

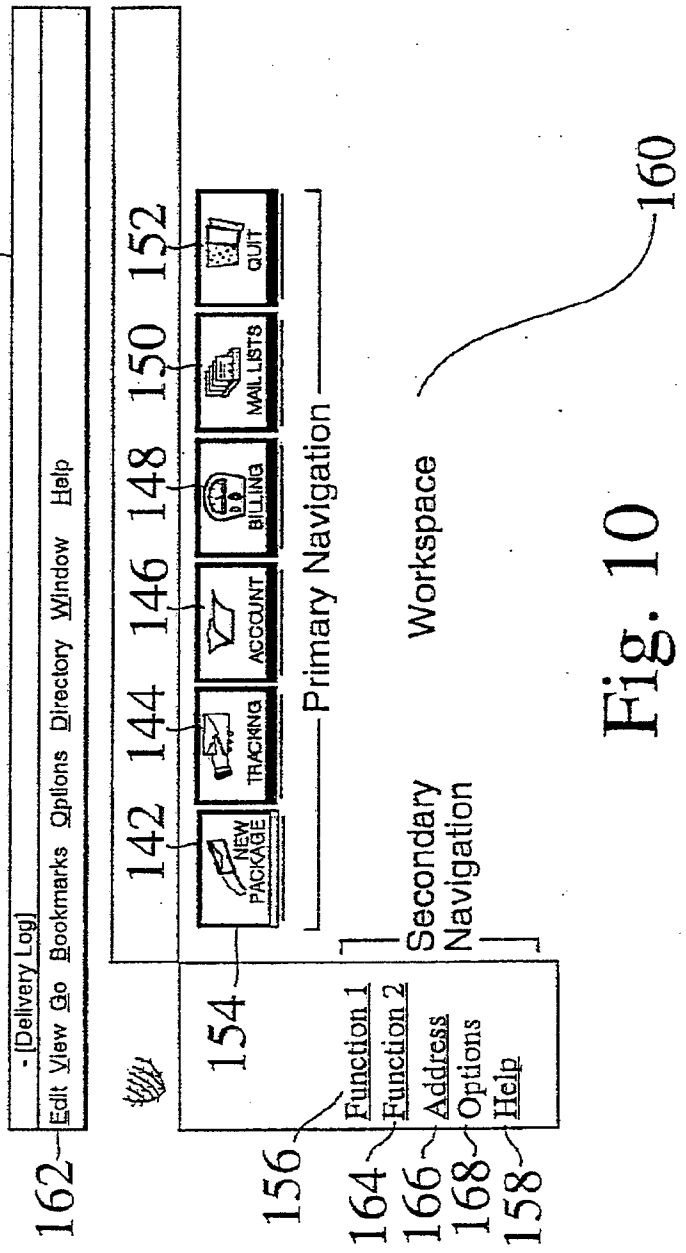

140
- [Delivery Log]
Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
Primary Navigation
154
Workspace
160
Function 1
Function 2
Address
Options
Help
Secondary Navigation
156
164
166
168
158

Fig. 10

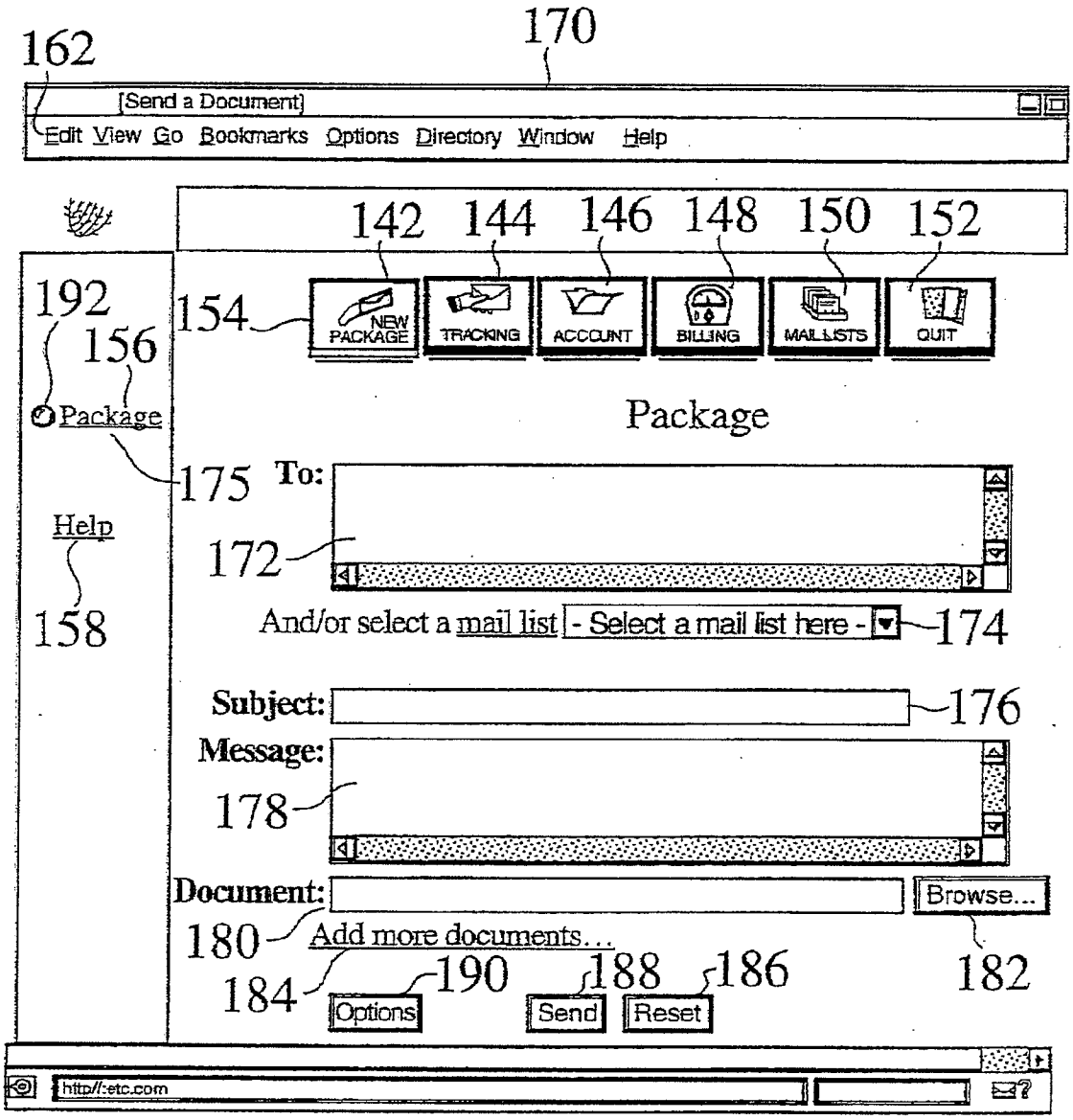

162
170
[Send a Document]
Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
192
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAILLISTS
QUIT
156
Package
Package
175
To:
Help
172
158
And/or select a mail list
- Select a mail list here -
174
Subject:
176
Message:
178
Document:
Browse...
180
Add more documents...
184
190
188
186
182
Options
Send
Reset
http://etc.com

Fig. 11

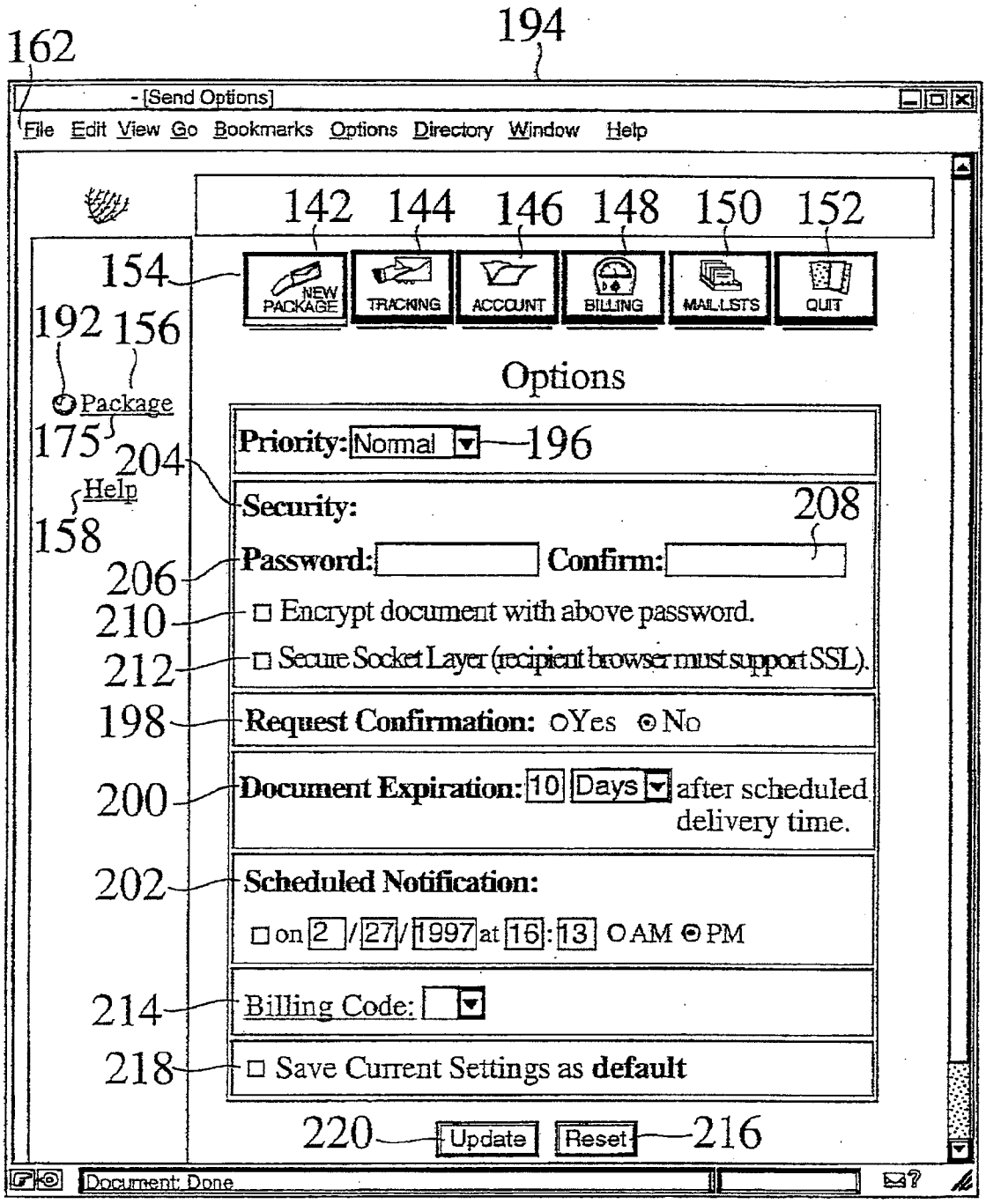

162
194
- [Send Options]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
Options
Package
175
204
Priority: Normal
196
Help
158
Security:
208
206
Password:
Confirm:
210
Encrypt document with above password.
212
Secure Socket Layer (recipient browser must support SSL).
198
Request Confirmation: Yes No
200
Document Expiration: 10 Days after scheduled delivery time.
202
Scheduled Notification:
on 2 / 27 / 1997 at 16 : 13 AM PM
214
Billing Code:
218
Save Current Settings as default
220
Update
Reset
216
Document: Done

Fig. 12

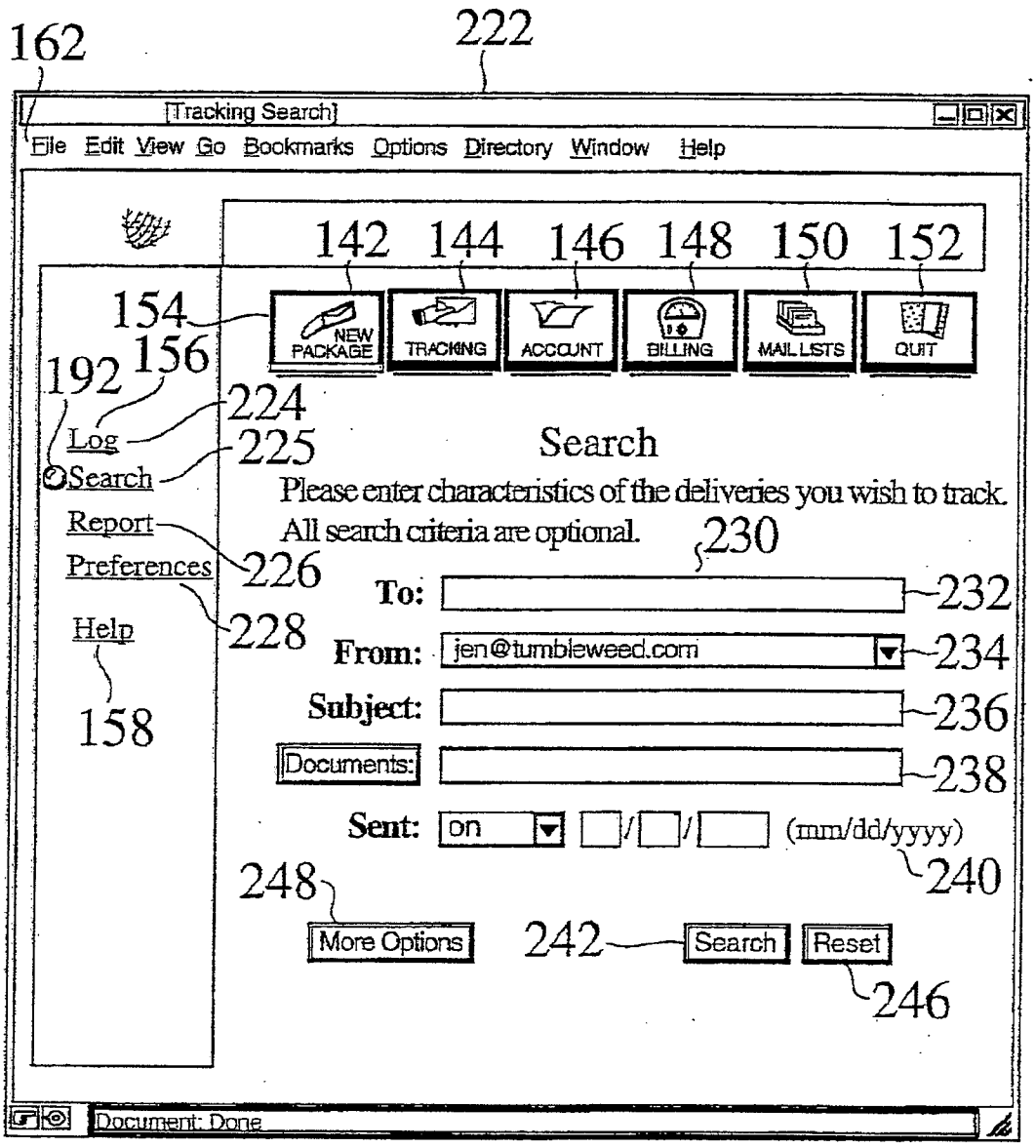

162
222
[Tracking Search]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
224
Log
225
Search
Report
226
Preferences
228
Help
158
Search
Please enter characteristics of the deliveries you wish to track.
All search criteria are optional.
230
To:
232
From:
jen@tumbleweed.com
234
Subject:
236
Documents:
238
Sent:
on
(mm/dd/yyyy)
240
248
More Options
242
Search
Reset
246
Document: Done

Fig. 13

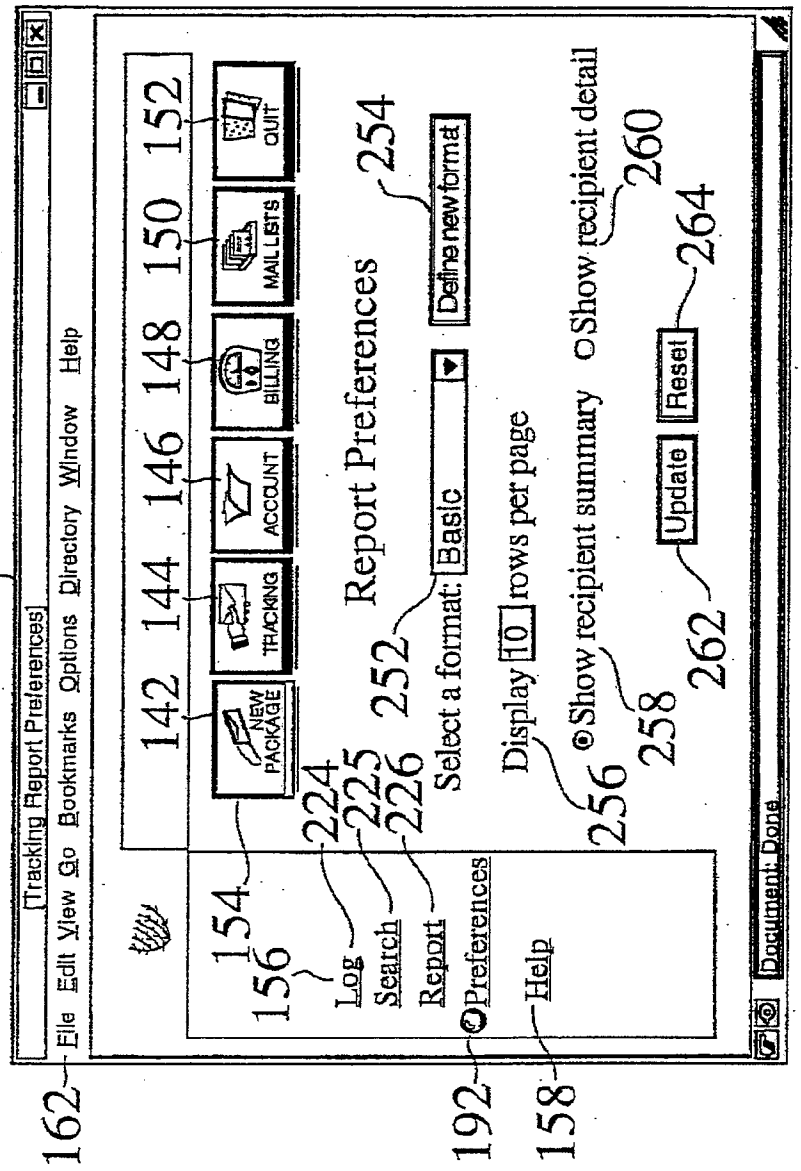

250
Tracking Report Preferences
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
154
156
Log
Search
Report
Preferences
Help
224
225
226
192
158
Report Preferences
252
254
Select a format: Basic
Define new format
Display 10 rows per page
Show recipient summary
Show recipient detail
256
258
260
262
Update
Reset
264
Document: Done

Fig. 14

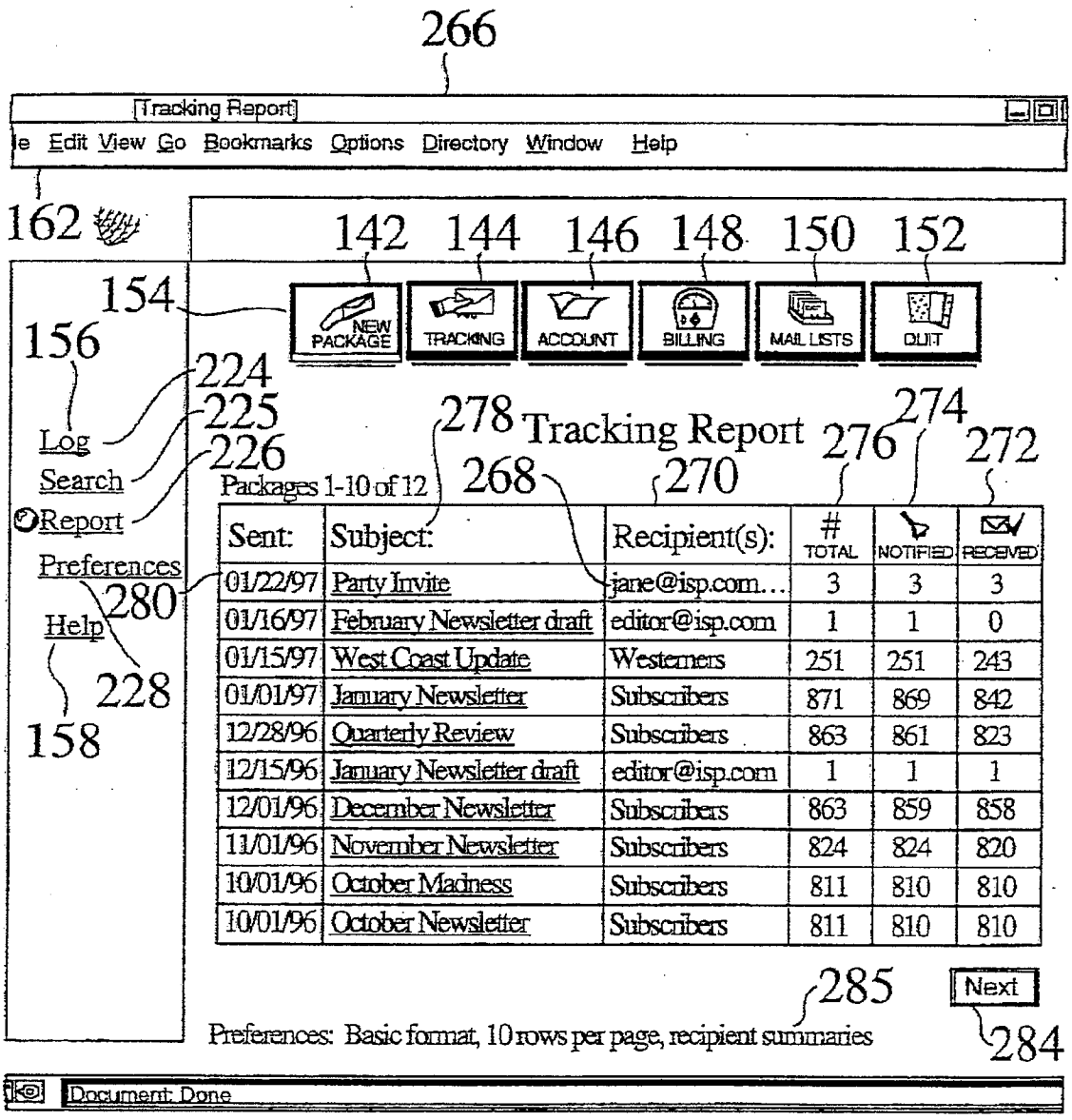

266
Tracking Report
le Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
156
224
225
226
Log
Search
Report
Preferences
Help
280
228
158
278
Tracking Report
276
274
272
Packages 1-10 of 12
268
270
Sent:
Subject:
Recipient(s):
TOTAL
NOTIFIED
RECEIVED
01/22/97 Party Invite jane@isp.com... 3 3 3
01/16/97 February Newsletter draft editor@isp.com 1 1 0
01/15/97 West Coast Update Westerners 251 251 243
01/01/97 January Newsletter Subscribers 871 869 842
12/28/96 Quarterly Review Subscribers 863 861 823
12/15/96 January Newsletter draft editor@isp.com 1 1 1
12/01/96 December Newsletter Subscribers 863 859 858
11/01/96 November Newsletter Subscribers 824 824 820
10/01/96 October Madness Subscribers 811 810 810
10/01/96 October Newsletter Subscribers 811 810 810
285
Next
284
Preferences: Basic format, 10 rows per page, recipient summaries
Document: Done

Fig. 15

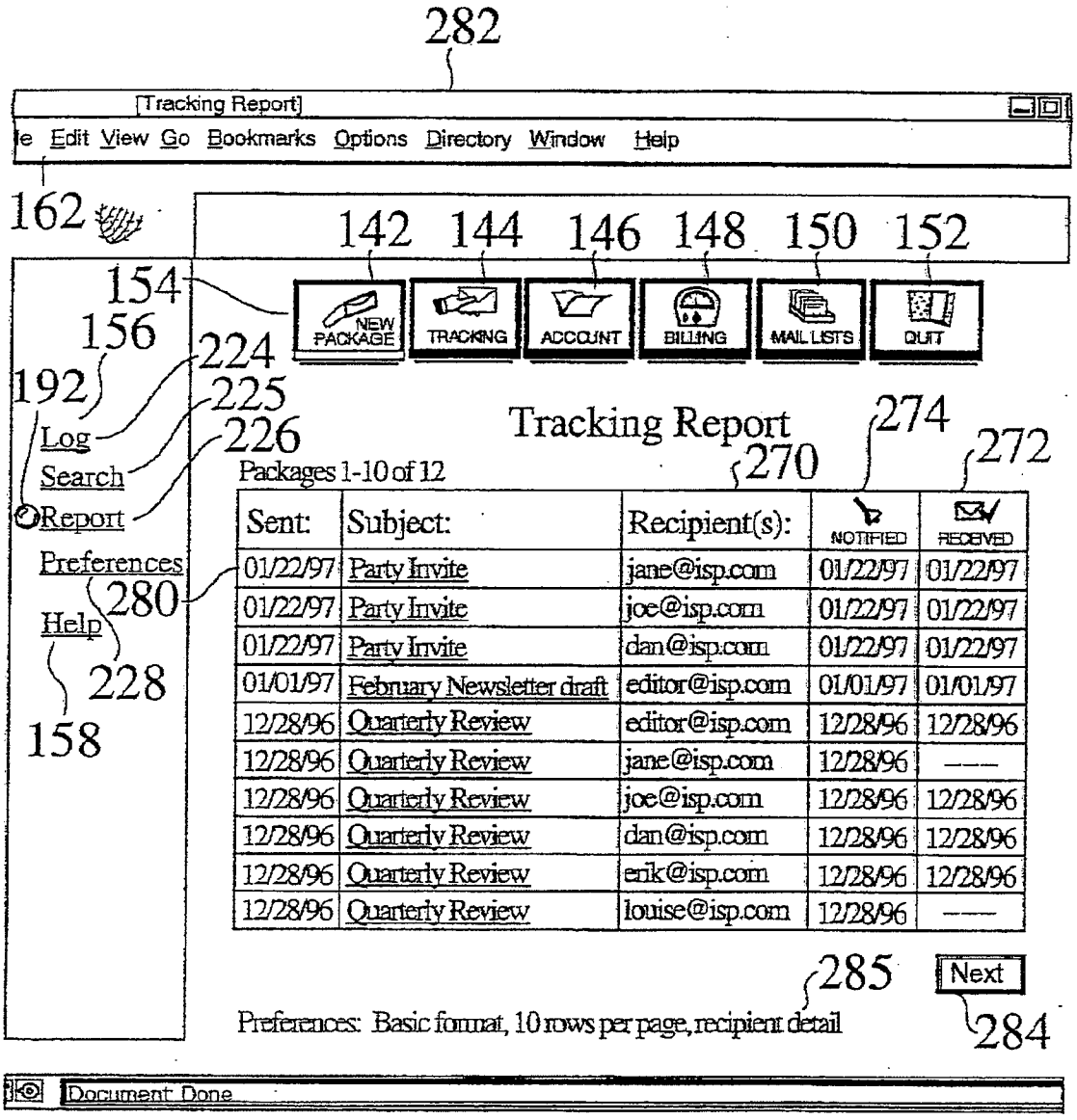

282
[Tracking Report]
le Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
154
156
192
224
225
226
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
Log
Search
Report
Preferences
Help
280
228
158
Tracking Report
274
270
272
Packages 1-10 of 12
Sent: Subject: Recipient(s): NOTIFIED RECEIVED
01/22/97 Party Invite jane@isp.com 01/22/97 01/22/97
01/22/97 Party Invite joe@isp.com 01/22/97 01/22/97
01/22/97 Party Invite dan@isp.com 01/22/97 01/22/97
01/01/97 February Newsletter draft editor@isp.com 01/01/97 01/01/97
12/28/96 Quarterly Review editor@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review jane@isp.com 12/28/96 ---
12/28/96 Quarterly Review joe@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review dan@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review erik@isp.com 12/28/96 12/28/96
12/28/96 Quarterly Review louise@isp.com 12/28/96 ---
285
Next
284
Preferences: Basic format, 10 rows per page, recipient detail
Document Done

Fig. 16

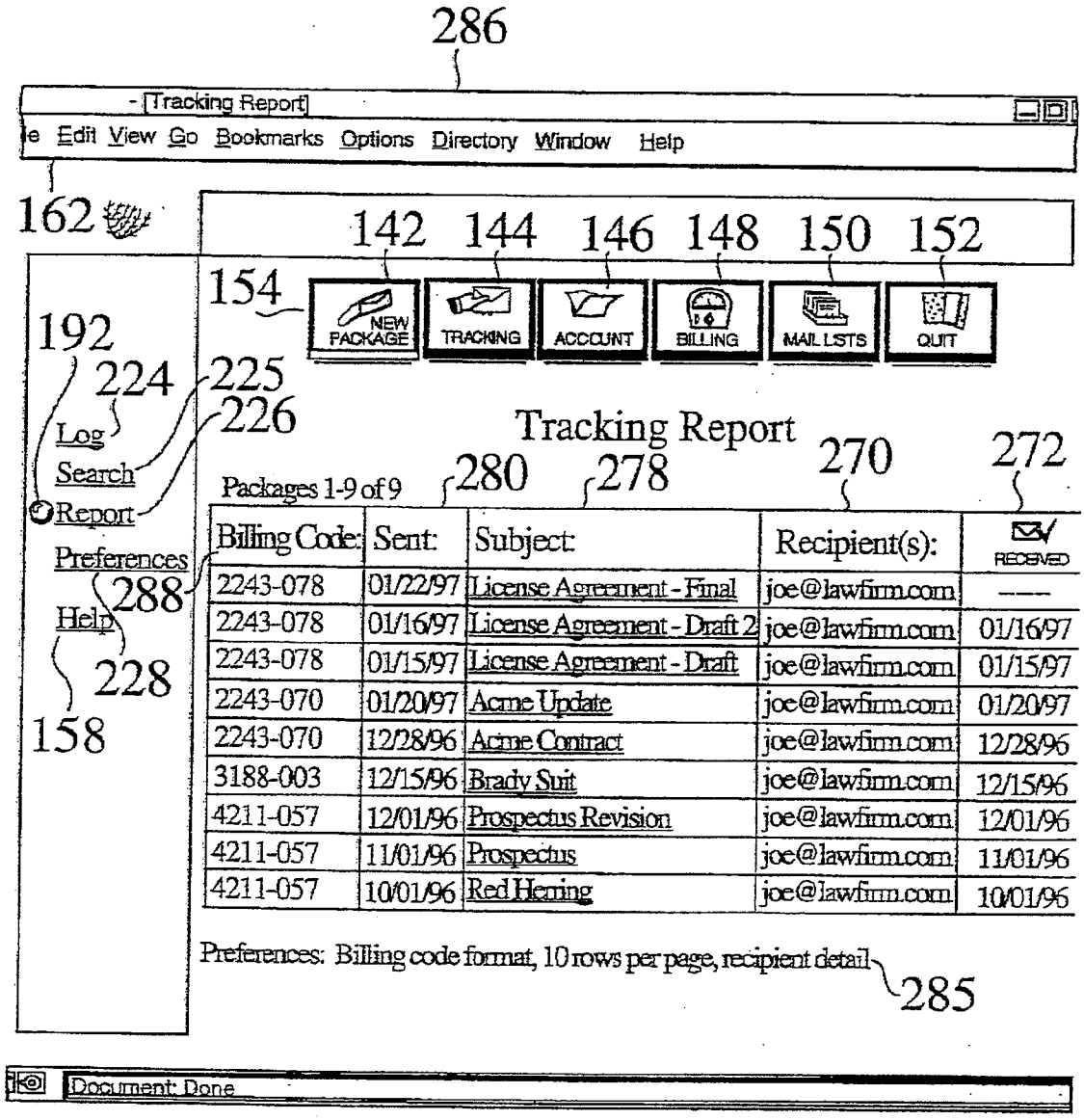

286
- [Tracking Report]
le Edit View Go Bookmarks Options Directory Window Help
162
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192
224
225
226
Log
Search
Report
Preferences
288
Help
228
158
Tracking Report
Packages 1-9 of 9
280
278
270
272
Billing Code:
Sent:
Subject:
Recipient(s):
RECEIVED
2243-078 01/22/97 License Agreement - Final joe@lawfirm.com ----
2243-078 01/16/97 License Agreement - Draft 2 joe@lawfirm.com 01/16/97
2243-078 01/15/97 License Agreement - Draft joe@lawfirm.com 01/15/97
2243-070 01/20/97 Acme Update joe@lawfirm.com 01/20/97
2243-070 12/28/96 Acme Contract joe@lawfirm.com 12/28/96
3188-003 12/15/96 Brady Suit joe@lawfirm.com 12/15/96
4211-057 12/01/96 Prospectus Revision joe@lawfirm.com 12/01/96
4211-057 11/01/96 Prospectus joe@lawfirm.com 11/01/96
4211-057 10/01/96 Red Herring joe@lawfirm.com 10/01/96
Preferences: Billing code format, 10 rows per page, recipient detail
285
Document: Done

Fig. 17

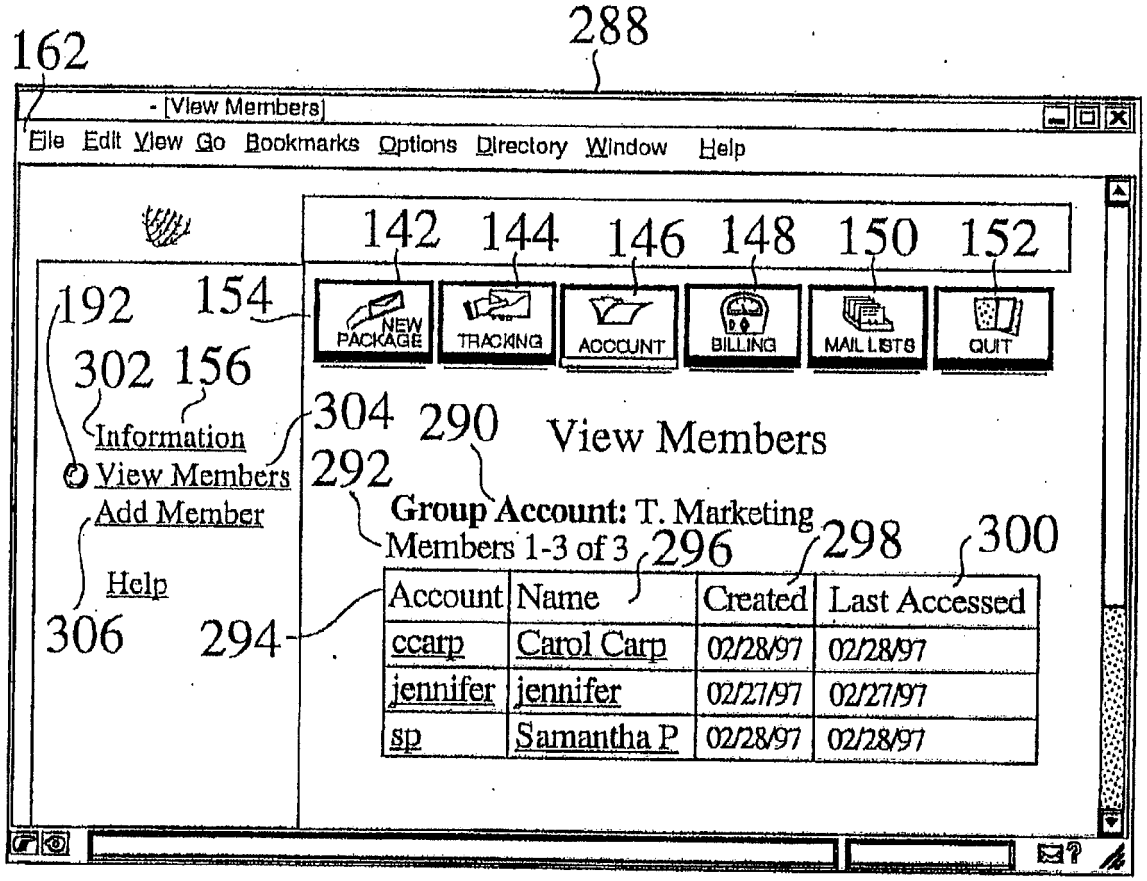

162
288
- [View Members]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 154
302 156
Information
View Members
Add Member
Help
306 294
304 290 View Members
292
Group Account: T. Marketing
Members 1-3 of 3
296 298 300
Account | Name | Created | Last Accessed
ccarp | Carol Carp | 02/28/97 | 02/28/97
jennifer | jennifer | 02/27/97 | 02/27/97
sp | Samantha P | 02/28/97 | 02/28/97

Fig. 18

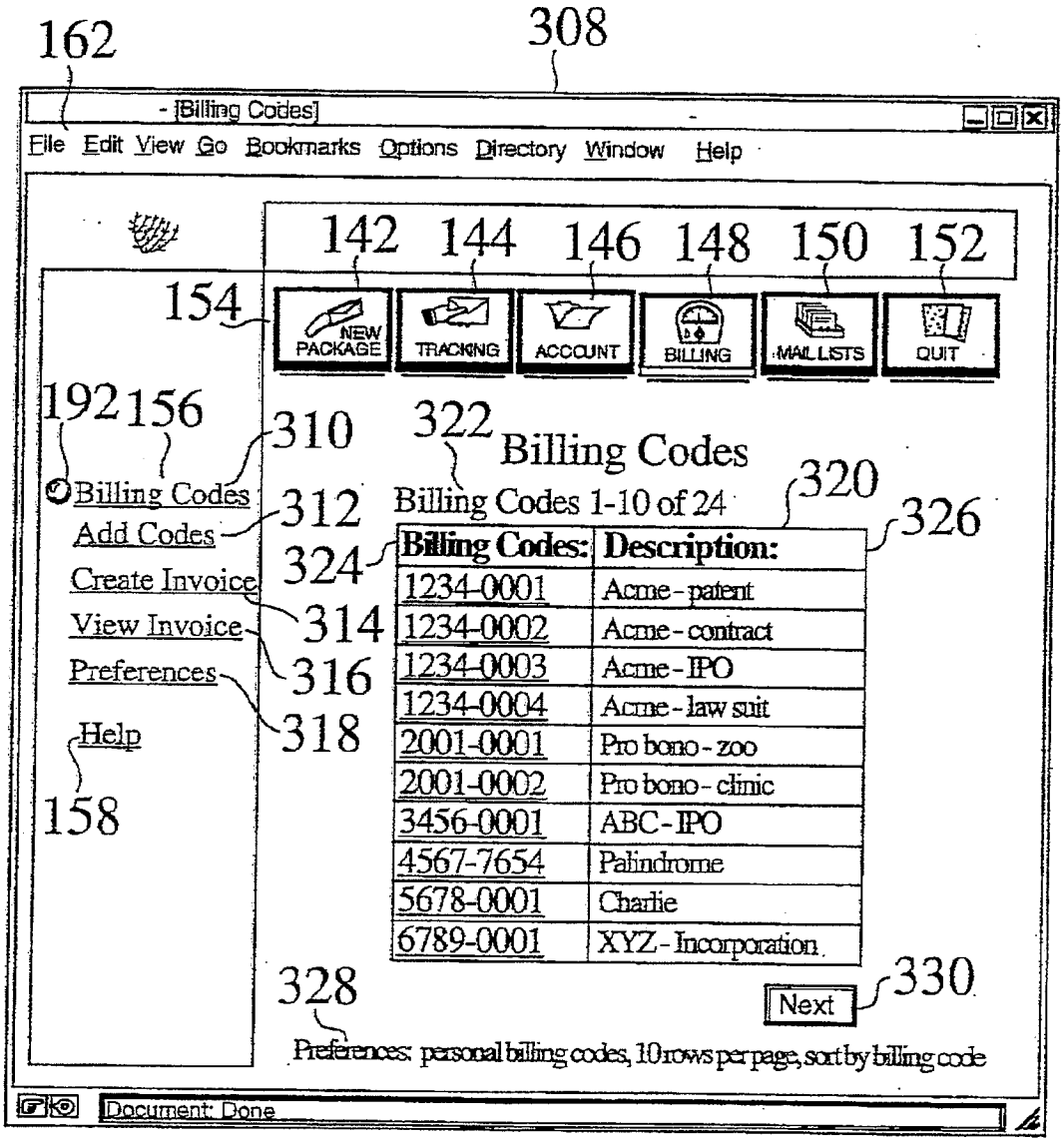

162
308
- [Billing Codes]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
310
322
Billing Codes
Billing Codes
312
Billing Codes 1-10 of 24
320
326
Add Codes
324
Billing Codes: Description:
Create Invoice
1234-0001 Acme - patent
314
View Invoice
1234-0002 Acme - contract
316
1234-0003 Acme - IPO
Preferences
1234-0004 Acme - law suit
318
2001-0001 Pro bono - zoo
Help
2001-0002 Pro bono - clinic
158
3456-0001 ABC - IPO
4567-7654 Palindrome
5678-0001 Charlie
6789-0001 XYZ - Incorporation
328
330
Next
Preferences: personal billing codes, 10 rows per page, sort by billing code
Document: Done

Fig. 19

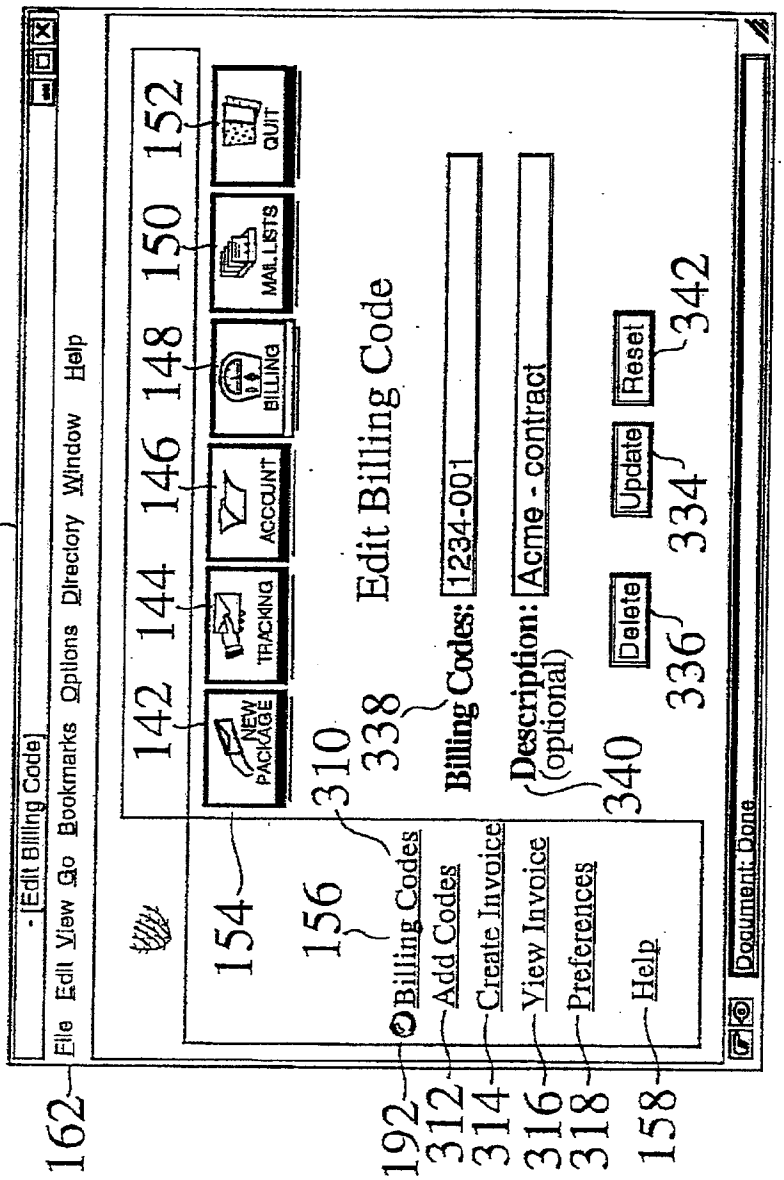

332
[Edit Billing Code]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAILLISTS
QUIT
154
156
310
338
Edit Billing Code
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
Billing Codes: 1234-001
Description: (optional) Acme - contract
340
Delete
Update
Reset
336
334
342
Document: Done
162
192
312
314
316
318
158

Fig. 20

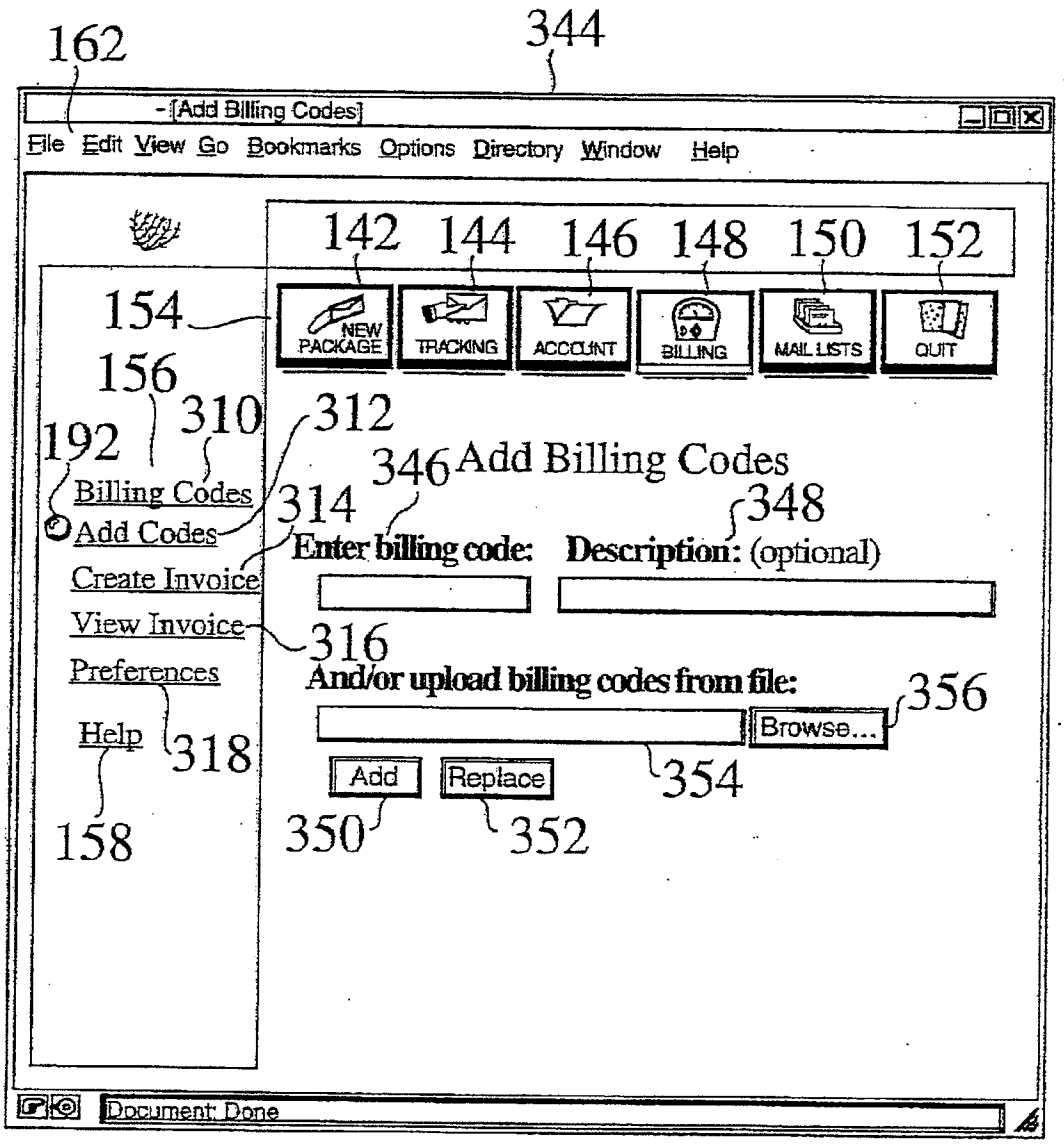

162
344
- [Add Billing Codes]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
156
310
312
192
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
318
158
346 Add Billing Codes
314
348
Enter billing code:
Description: (optional)
316
And/or upload billing codes from file:
356
Browse...
354
Add
Replace
350
352
Document: Done

Fig. 21

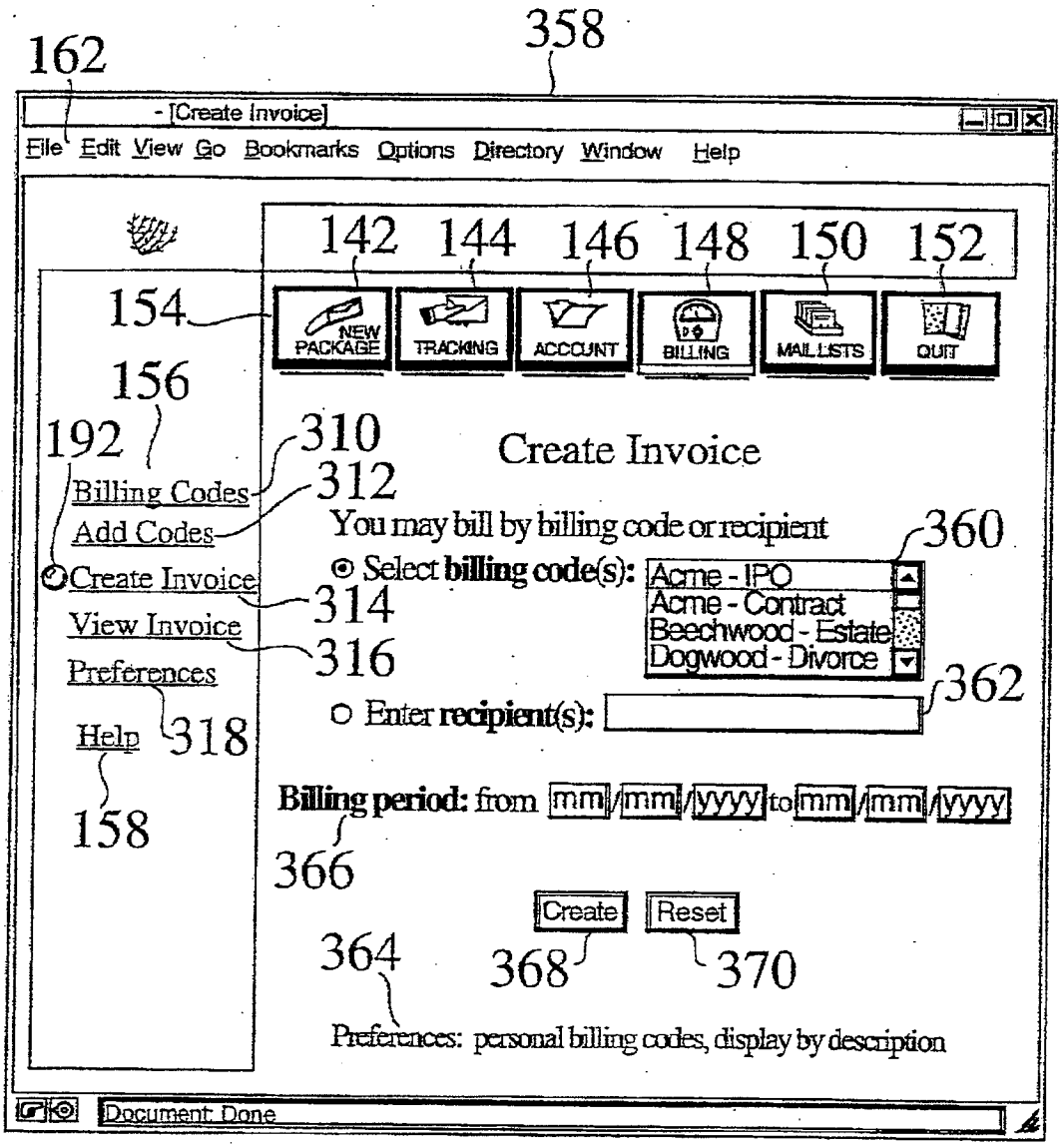

162
358
- [Create Invoice]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAILLISTS
QUIT
156
192
310
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
314
316
318
158
Create Invoice
You may bill by billing code or recipient
360
Select billing code(s):
Acme - IPO
Acme - Contract
Beechwood - Estate
Dogwood - Divorce
362
Enter recipient(s):
Billing period: from mm/mm/yyyy to mm/mm/yyyy
366
Create
Reset
364
368
370
Preferences: personal billing codes, display by description
Document: Done

Fig. 22

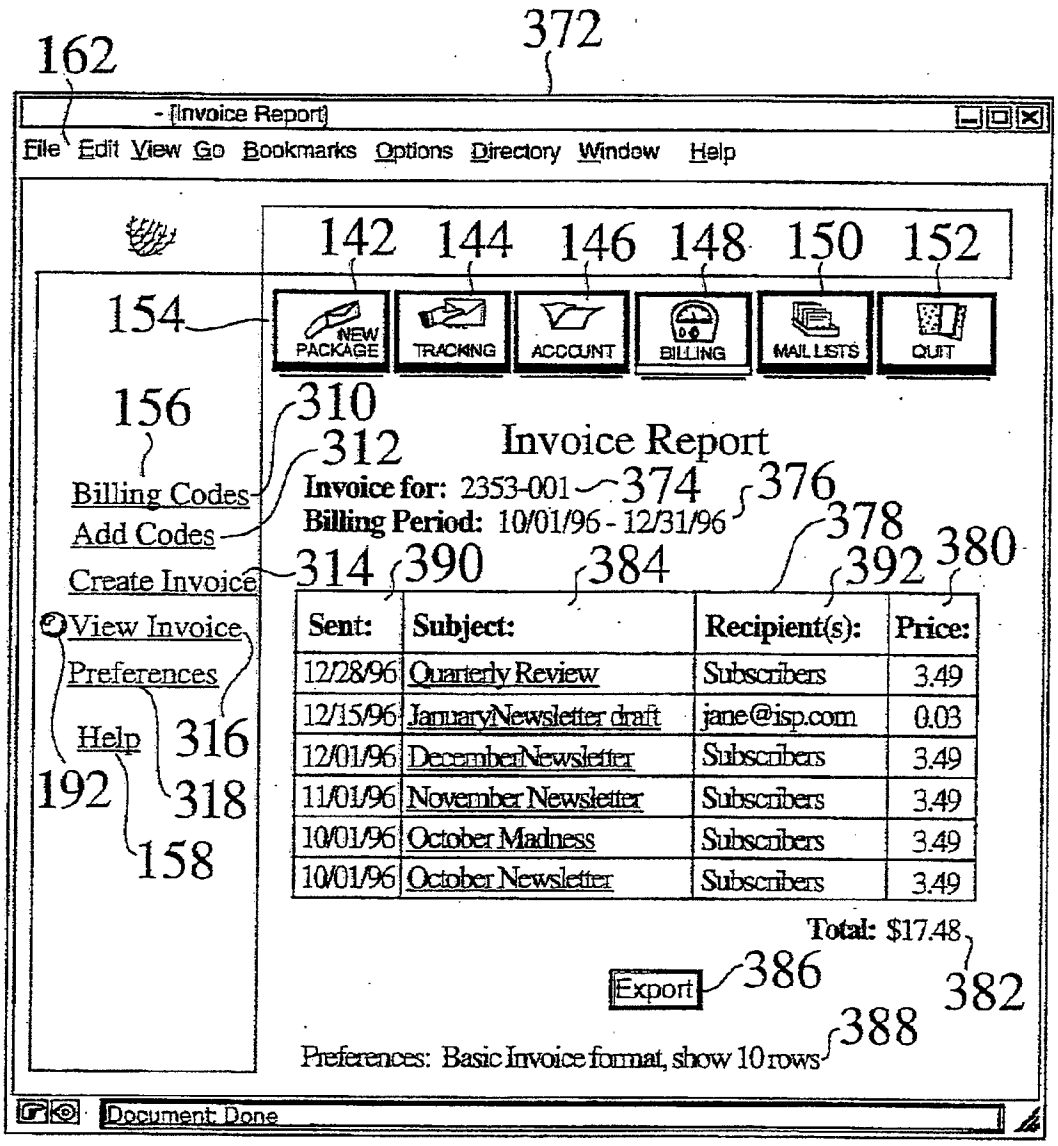

162
372
- [Invoice Report]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
156
310
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
192
158
316
318
314
Invoice Report
Invoice for: 2353-001
374
376
Billing Period: 10/01/96 - 12/31/96
378
380
390
384
392
Sent: | Subject: | Recipient(s): | Price:
12/28/96 | Quarterly Review | Subscribers | 3.49
12/15/96 | JanuaryNewsletter draft | jane@isp.com | 0.03
12/01/96 | DecemberNewsletter | Subscribers | 3.49
11/01/96 | November Newsletter | Subscribers | 3.49
10/01/96 | October Madness | Subscribers | 3.49
10/01/96 | October Newsletter | Subscribers | 3.49
Total: $17.48
382
Export
386
388
Preferences: Basic Invoice format, show 10 rows
Document: Done

Fig. 23

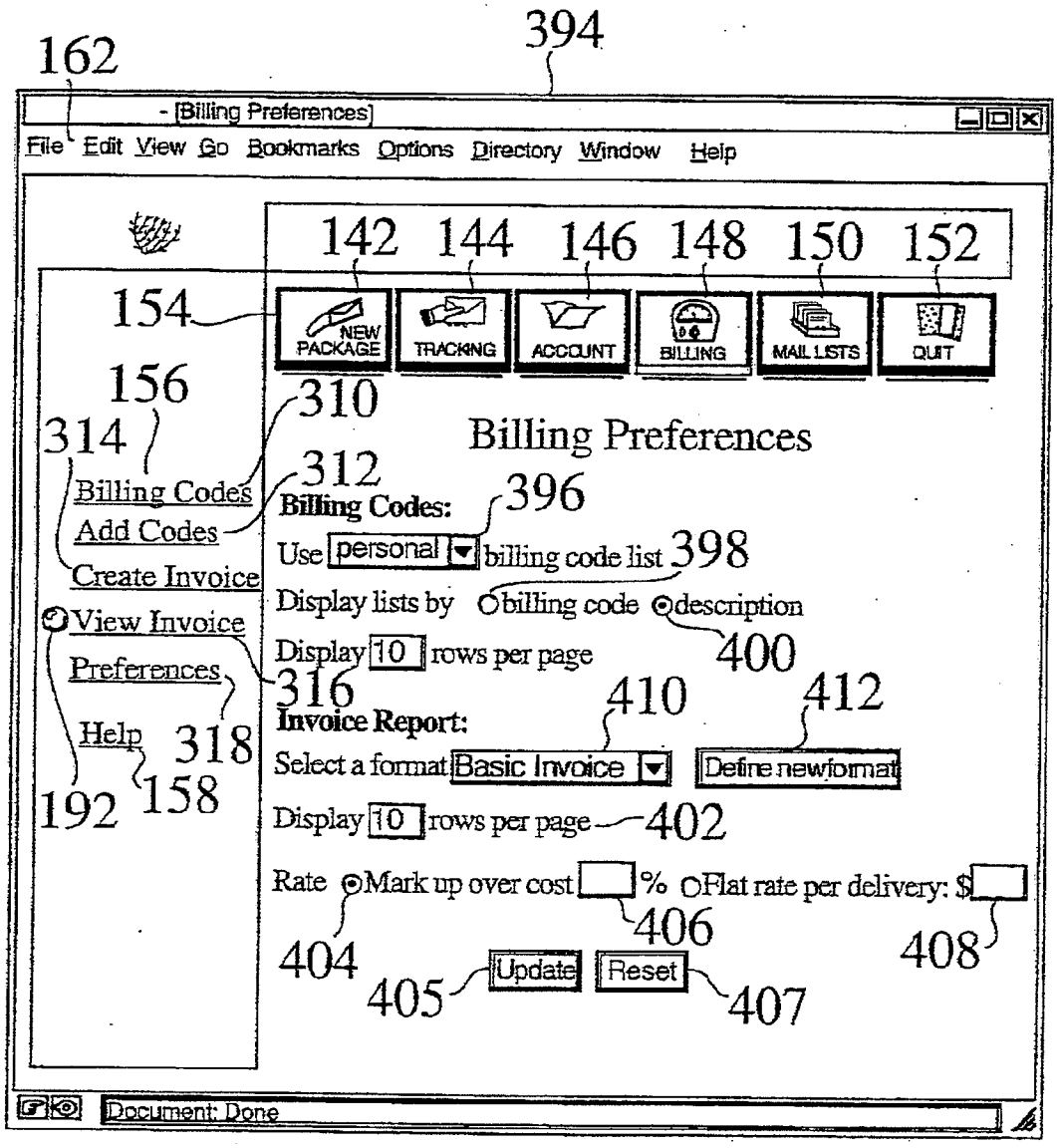

162
394
- [Billing Preferences]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
156
310
314
Billing Preferences
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
192
158
318
316
Billing Codes:
396
Use personal billing code list 398
Display lists by billing code description
400
Display 10 rows per page
Invoice Report:
410
412
Select a format Basic Invoice
Define newformat
Display 10 rows per page
402
Rate Mark up over cost % Flat rate per delivery: $
404
406
408
405
Update
Reset
407
Document: Done

Fig. 24

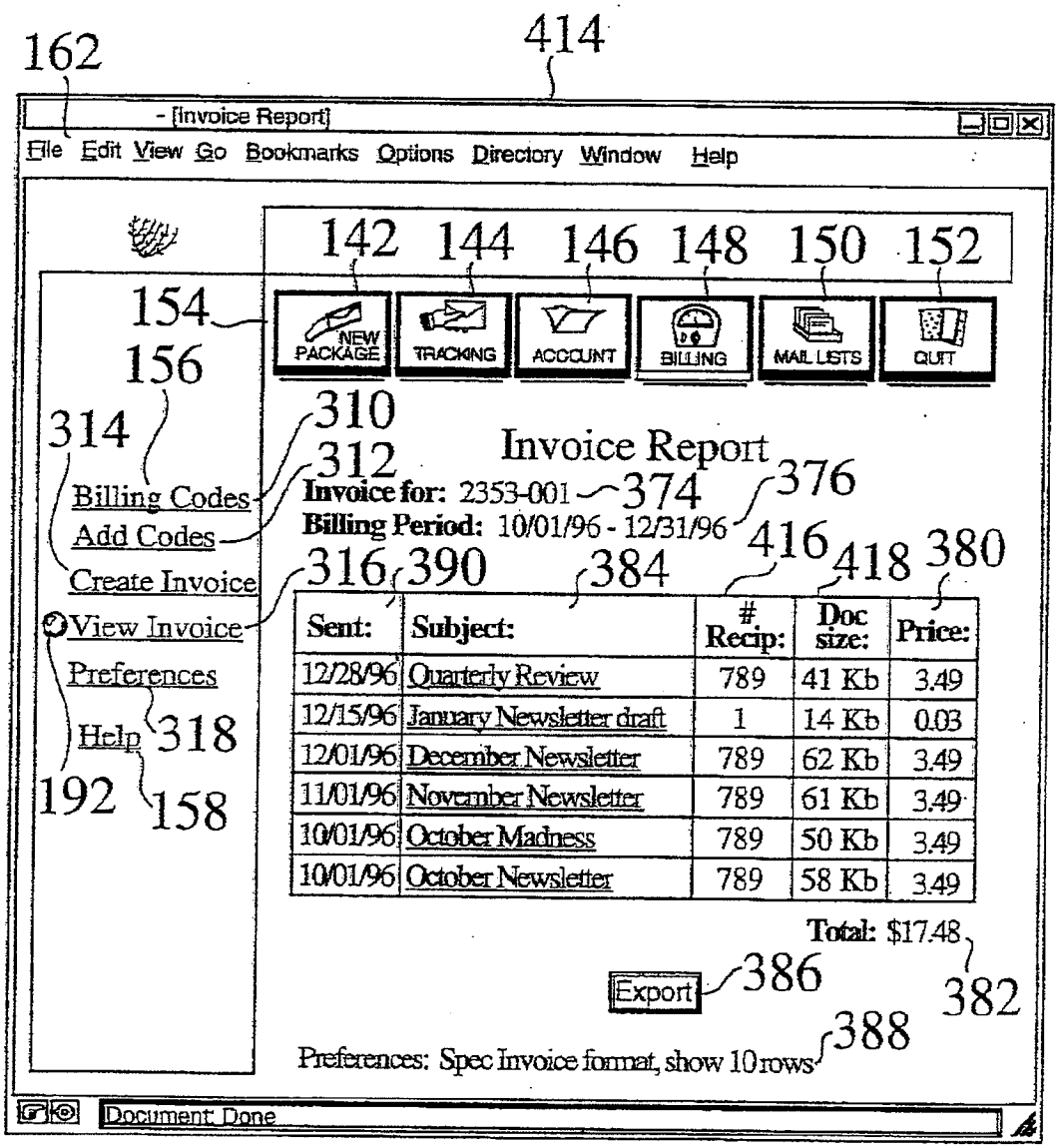

162
414
- [Invoice Report]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
156
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
314
310
312
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
192
158
318
Invoice Report
Invoice for: 2353-001
374
376
Billing Period: 10/01/96 - 12/31/96
316
390
384
416
418
380
Sent: | Subject: | # Recip: | Doc size: | Price:
12/28/96 | Quarterly Review | 789 | 41 Kb | 3.49
12/15/96 | January Newsletter draft | 1 | 14 Kb | 0.03
12/01/96 | December Newsletter | 789 | 62 Kb | 3.49
11/01/96 | November Newsletter | 789 | 61 Kb | 3.49
10/01/96 | October Madness | 789 | 50 Kb | 3.49
10/01/96 | October Newsletter | 789 | 58 Kb | 3.49
Total: $17.48
382
Export
386
388
Preferences: Spec Invoice format, show 10 rows
Document: Done

Fig. 25

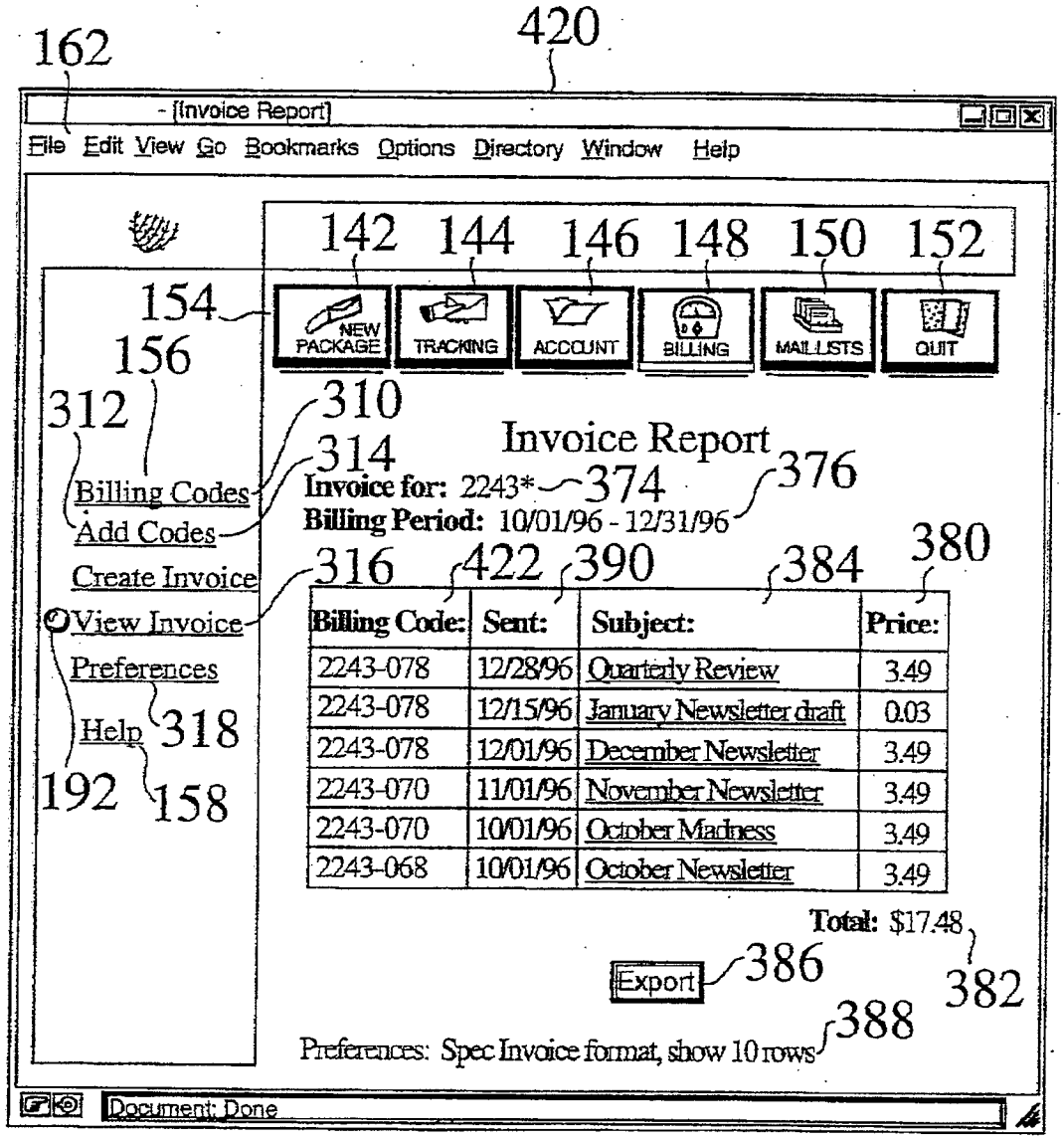

162
420
- [Invoice Report]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
156
312
310
314
316
422
390
384
380
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAILLISTS
QUIT
Billing Codes
Add Codes
Create Invoice
View Invoice
Preferences
Help
318
192
158
Invoice Report
Invoice for: 2243*
374
376
Billing Period: 10/01/96 - 12/31/96
Billing Code: | Sent: | Subject: | Price:
2243-078 | 12/28/96 | Quarterly Review | 3.49
2243-078 | 12/15/96 | January Newsletter draft | 0.03
2243-078 | 12/01/96 | December Newsletter | 3.49
2243-070 | 11/01/96 | November Newsletter | 3.49
2243-070 | 10/01/96 | October Madness | 3.49
2243-068 | 10/01/96 | October Newsletter | 3.49
Total: $17.48
382
Export
386
388
Preferences: Spec Invoice format, show 10 rows
Document: Done

Fig. 26

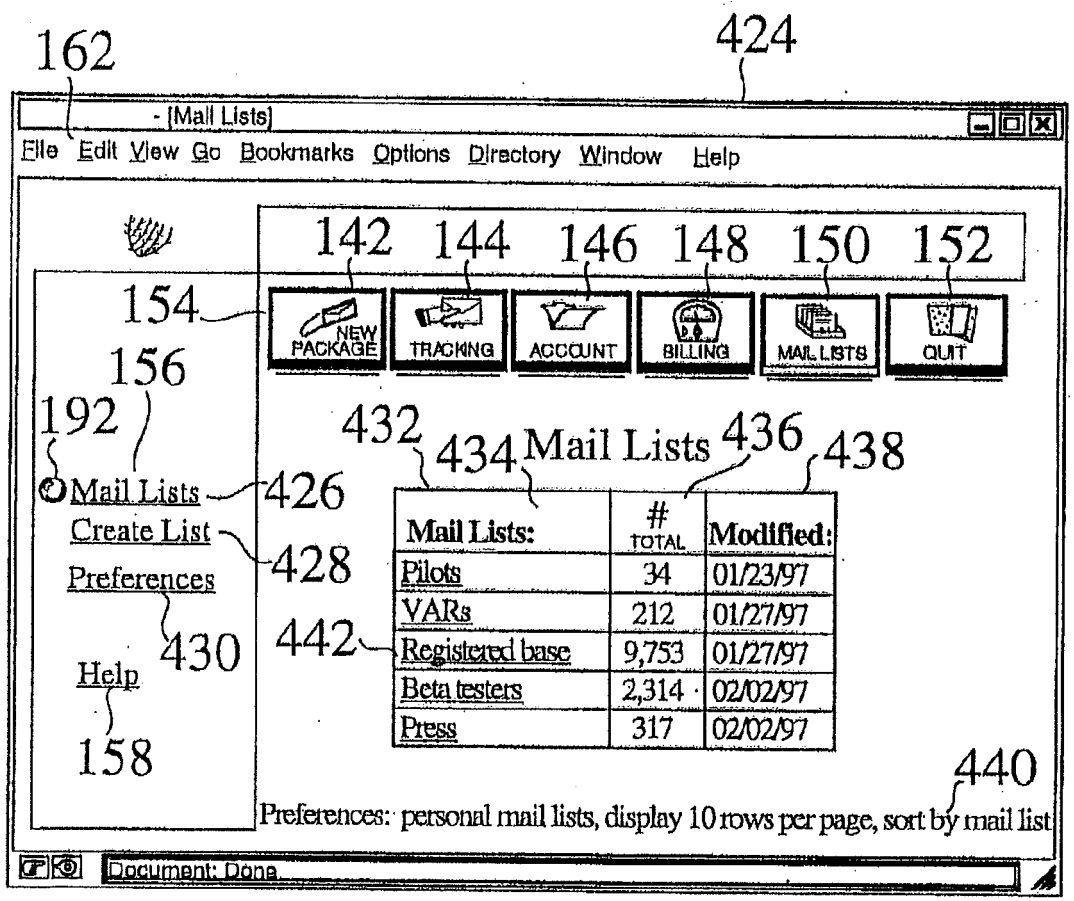


Fig. 27

特開平11-272594

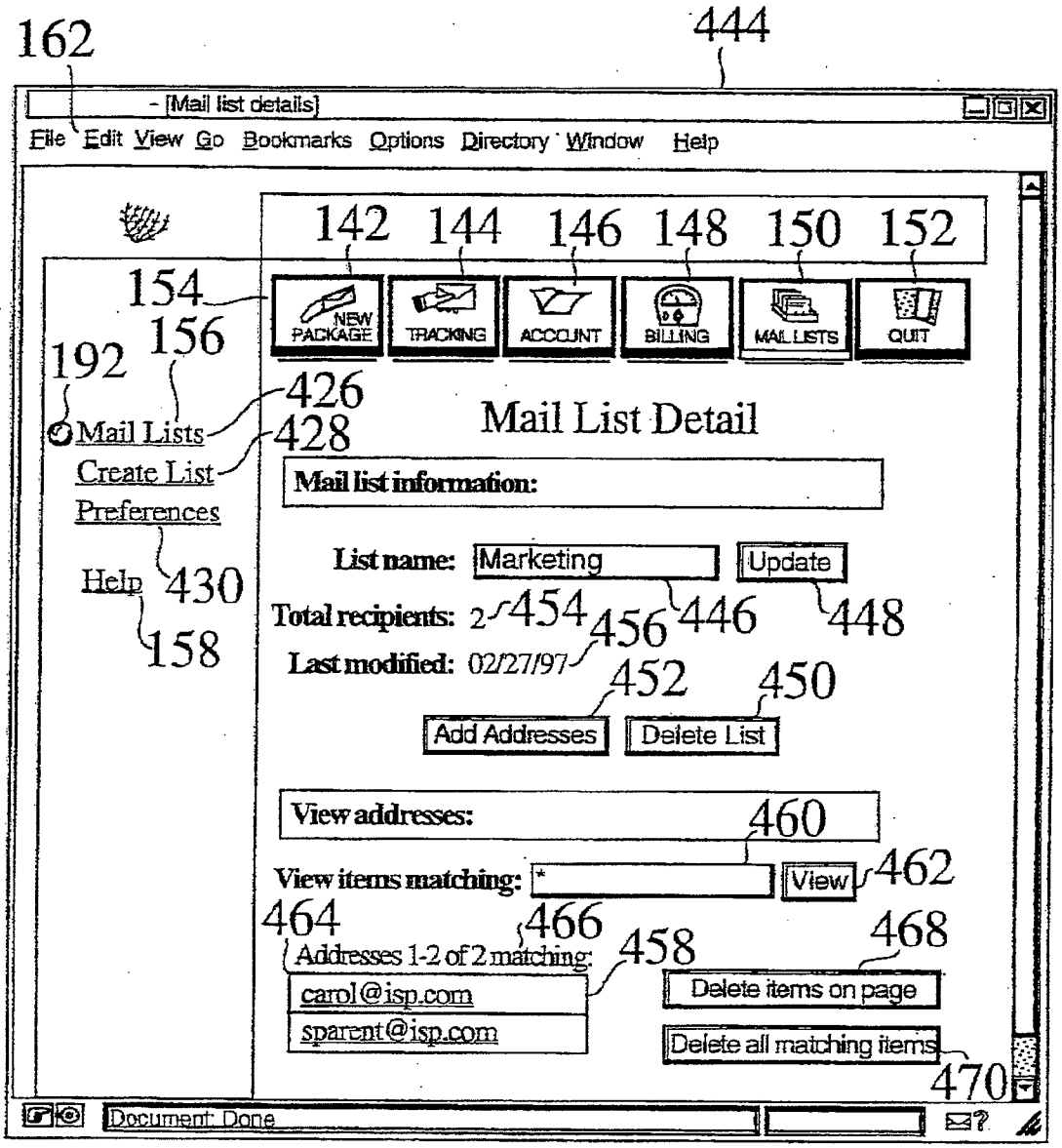

162
444
- [Mail list details]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
156
192
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
426
428
Mail Lists
Create List
Preferences
Help
430
158
Mail List Detail
Mail list information:
List name: Marketing
Update
446
448
Total recipients: 2
454
456
Last modified: 02/27/97
452
450
Add Addresses
Delete List
View addresses:
460
View items matching: *
View
462
464
466
Addresses 1-2 of 2 matching:
458
468
carol@isp.com
sparent@isp.com
Delete items on page
Delete all matching items
470
Document: Done

Fig. 28

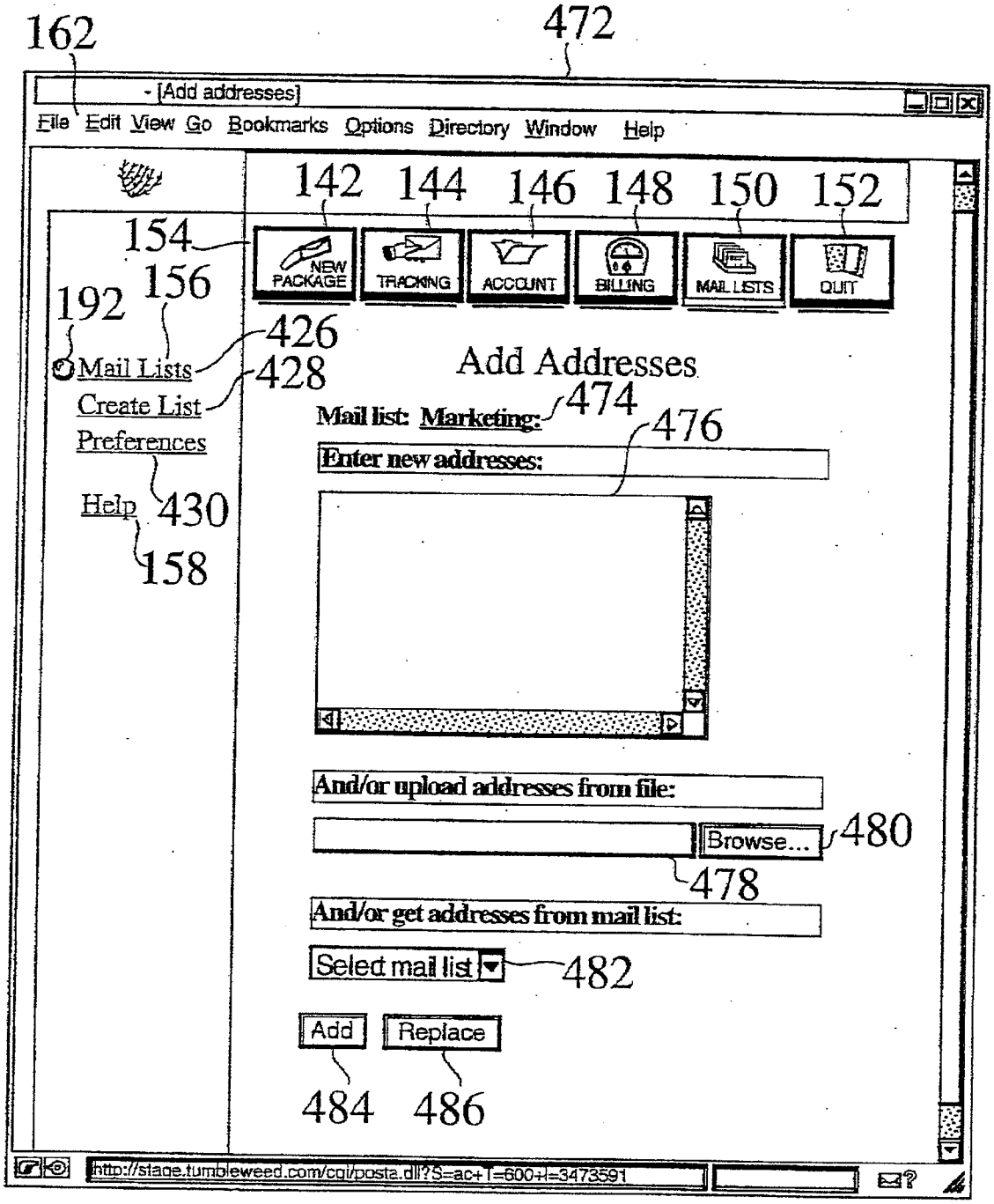

162
472
- [Add addresses]
File Edit View Go Bookmarks Options Directory Window Help
142 144 146 148 150 152
154
NEW PACKAGE
TRACKING
ACCOUNT
BILLING
MAIL LISTS
QUIT
192 156
426
Mail Lists
428
Create List
Preferences
Help 430
158
Add Addresses
Mail list: Marketing:
474
476
Enter new addresses:
And/or upload addresses from file:
Browse...
480
478
And/or get addresses from mail list:
Select mail list
482
Add
Replace
484 486
http://stage.tumbleweed.com/cgi/posta.dll?S=ac+T=600+I=3473591

Fig. 29

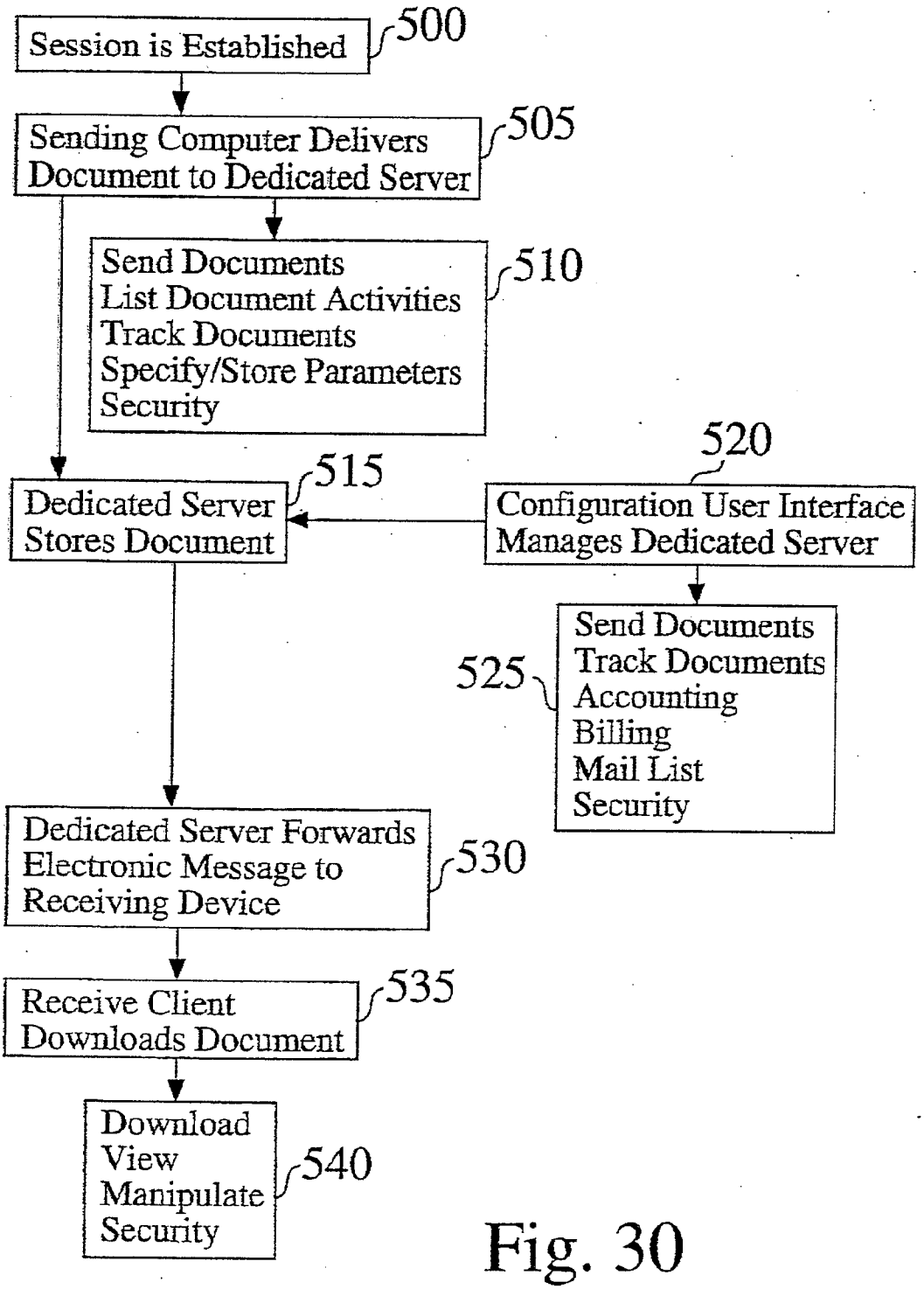

Session is Established
500
Sending Computer Delivers Document to Dedicated Server
505
Send Documents
List Document Activities
Track Documents
Specify/Store Parameters
Security
510
520
Dedicated Server Stores Document
515
Configuration User Interface Manages Dedicated Server
Send Documents
Track Documents
Accounting
Billing
Mail List
Security
525
Dedicated Server Forwards Electronic Message to Receiving Device
530
Receive Client Downloads Document
535
Download
View
Manipulate
Security
540

Fig. 30

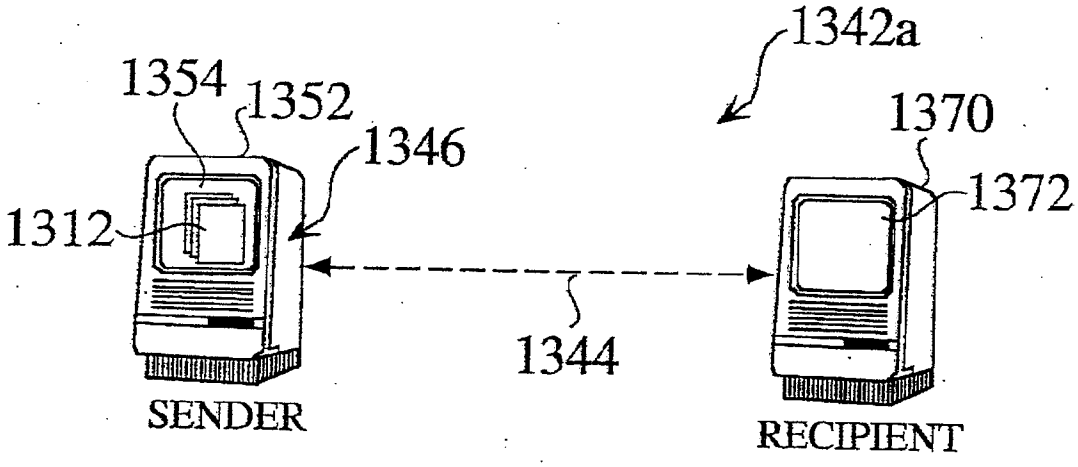

1342a
1354
1352
1346
1370
1372
1312
1344
SENDER
RECIPIENT

Fig. 31

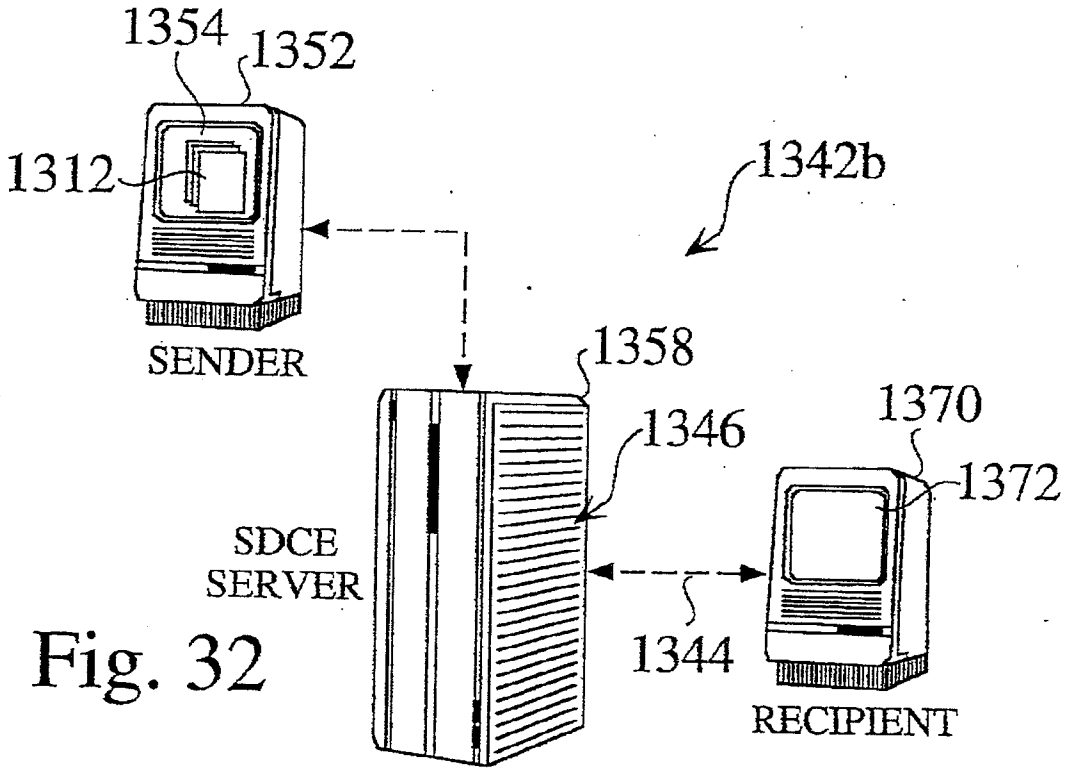

1354
1352
1342b
1312
SENDER
1358
1346
1370
1372
SDCE
SERVER
1344
RECIPIENT

Fig. 32

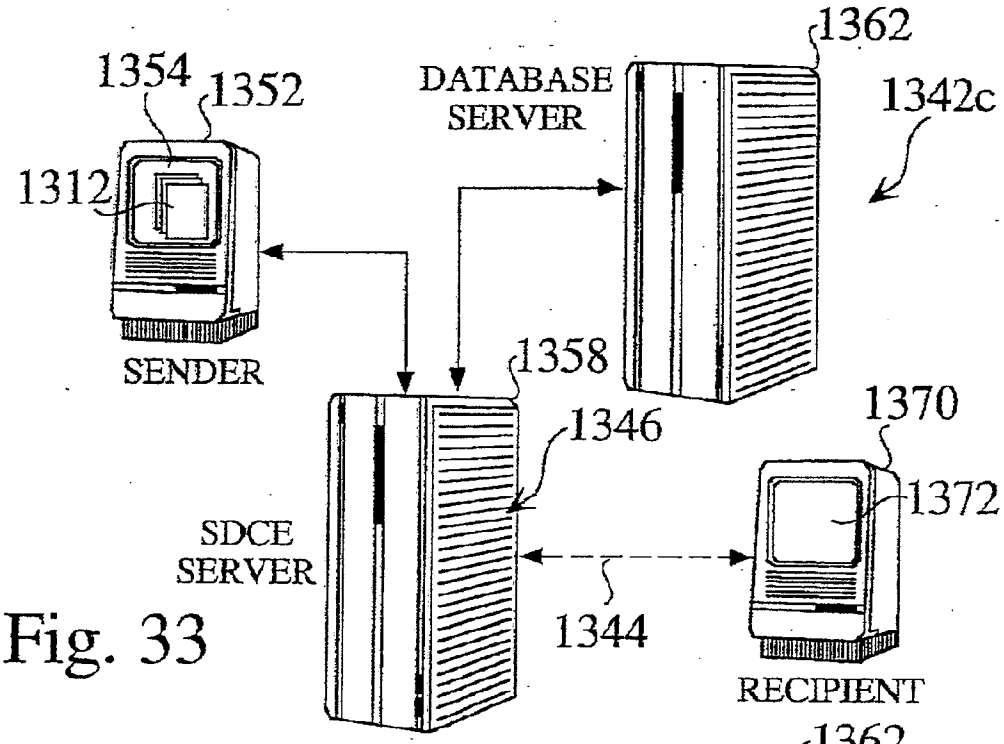

1362
1354
1352
DATABASE SERVER
1342c
1312
SENDER
1358
1346
1370
1372
SDCE SERVER
1344
RECIPIENT

Fig. 33

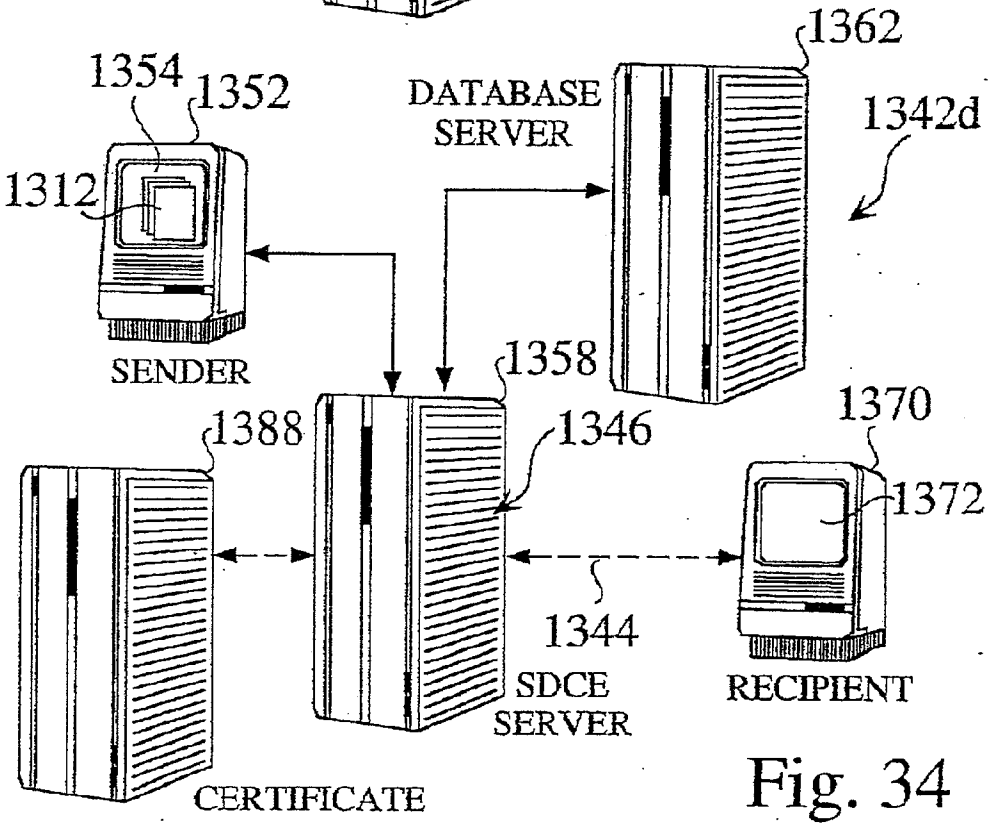

1362
1354
1352
DATABASE SERVER
1342d
1312
SENDER
1358
1388
1346
1370
1372
1344
SDCE SERVER
RECIPIENT
CERTIFICATE

Fig. 34

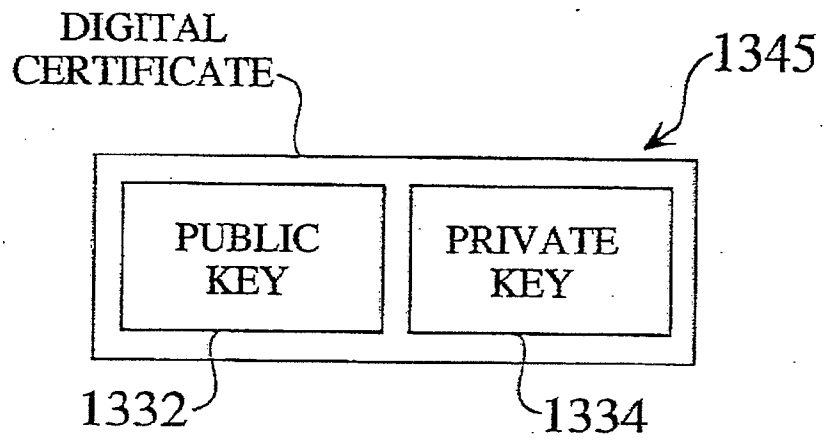

DIGITAL CERTIFICATE
1345
PUBLIC KEY
PRIVATE KEY
1332
1334

Fig. 35

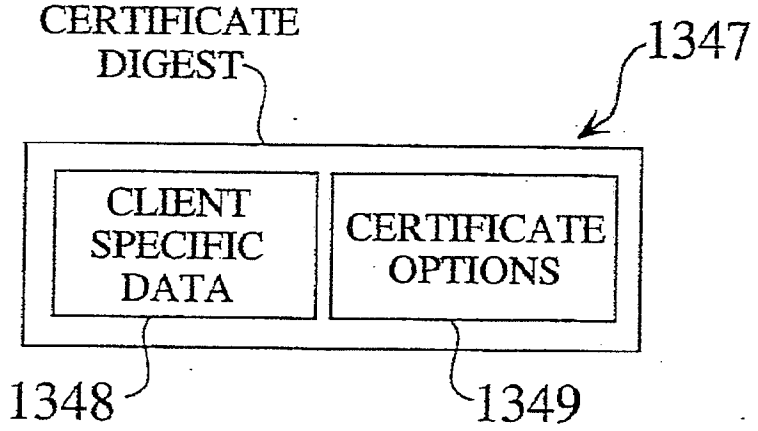

CERTIFICATE DIGEST
1347
CLIENT SPECIFIC DATA
CERTIFICATE OPTIONS
1348
1349

Fig. 36

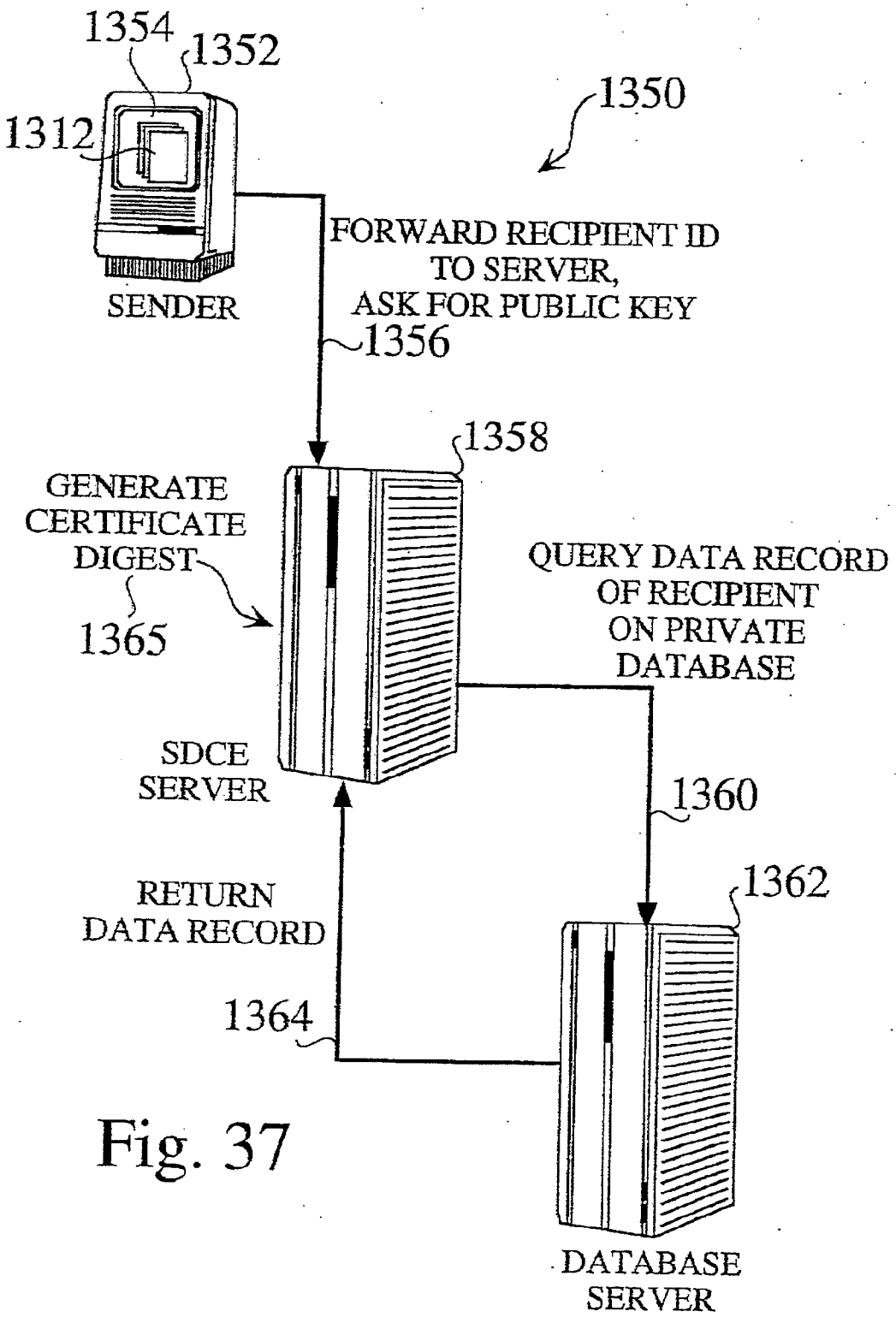

1354
1352
1312
1350
SENDER
FORWARD RECIPIENT ID
TO SERVER,
ASK FOR PUBLIC KEY
1356
1358
GENERATE
CERTIFICATE
DIGEST
1365
QUERY DATA RECORD
OF RECIPIENT
ON PRIVATE
DATABASE
SDCE
SERVER
1360
1362
RETURN
DATA RECORD
1364
DATABASE
SERVER

Fig. 37

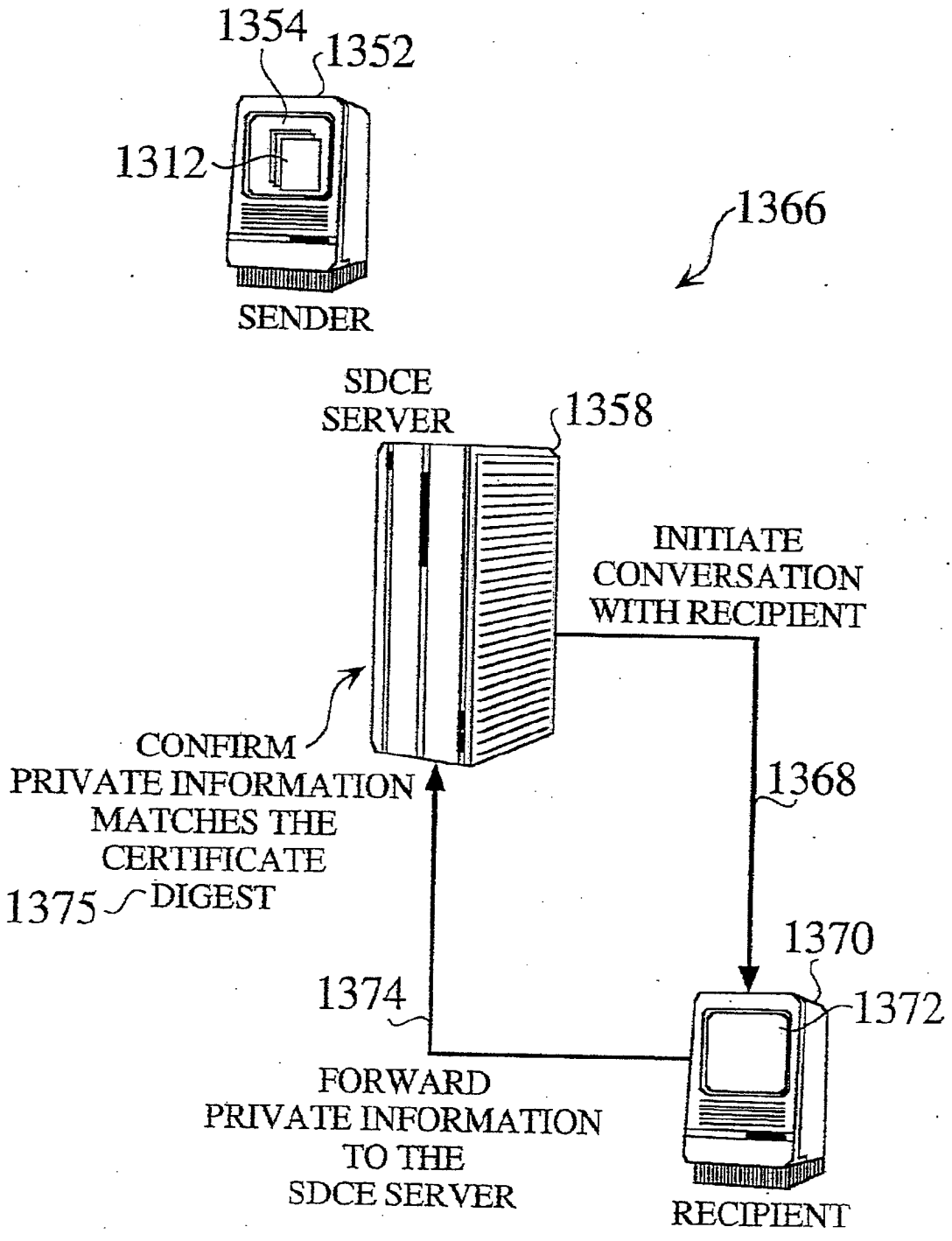

1354
1352
1312
SENDER
1366
SDCE
SERVER
1358
INITIATE
CONVERSATION
WITH RECIPIENT
CONFIRM
PRIVATE INFORMATION
MATCHES THE
CERTIFICATE
1375 DIGEST
1368
1370
1374
1372
FORWARD
PRIVATE INFORMATION
TO THE
SDCE SERVER
RECIPIENT

Fig. 38

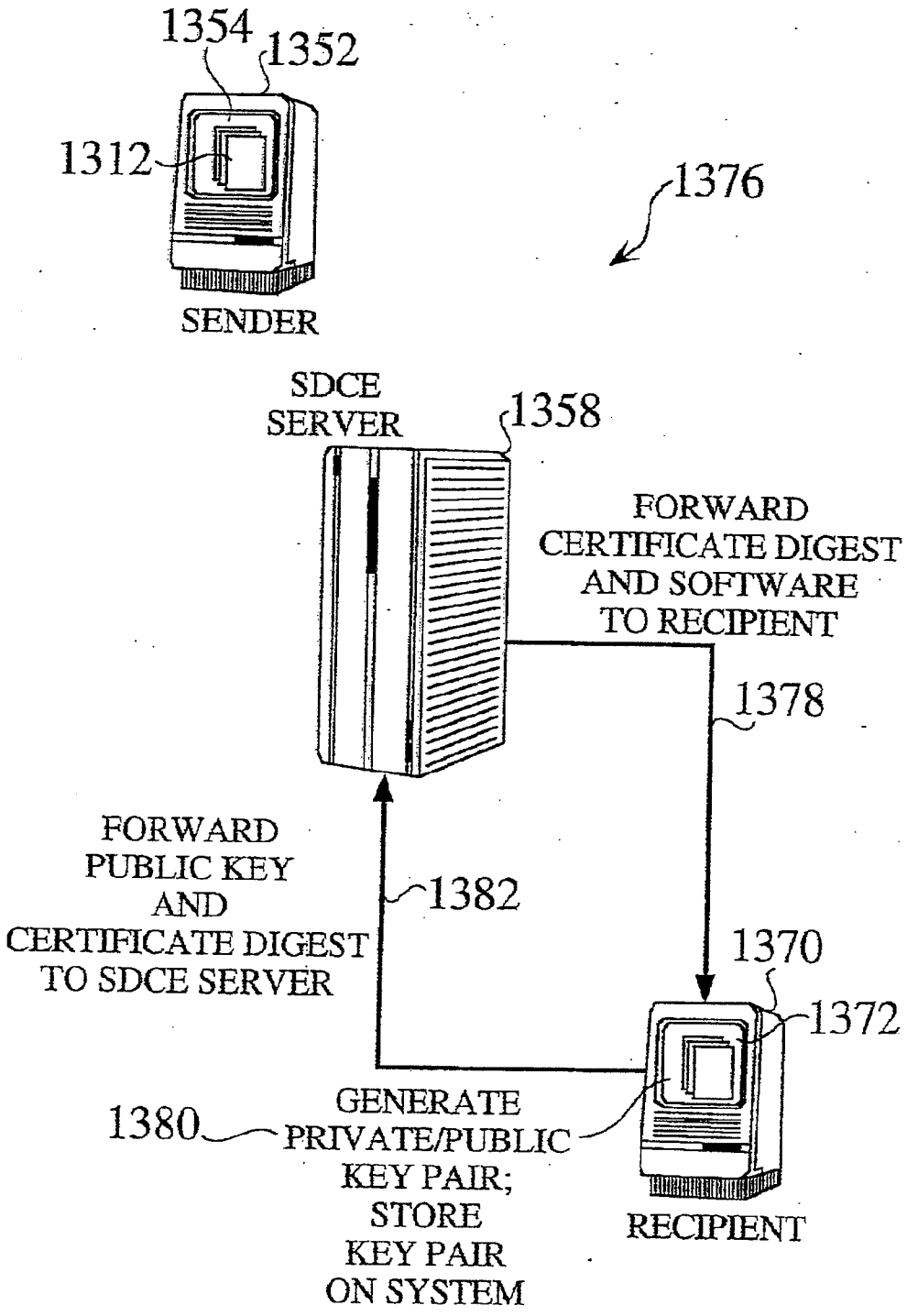

1354
1352
1312
1376
SENDER
SDCE
SERVER
1358
FORWARD
CERTIFICATE DIGEST
AND SOFTWARE
TO RECIPIENT
1378
FORWARD
PUBLIC KEY
AND
CERTIFICATE DIGEST
TO SDCE SERVER
1382
1370
1372
1380
GENERATE
PRIVATE/PUBLIC
KEY PAIR;
STORE
KEY PAIR
ON SYSTEM
RECIPIENT

Fig. 39

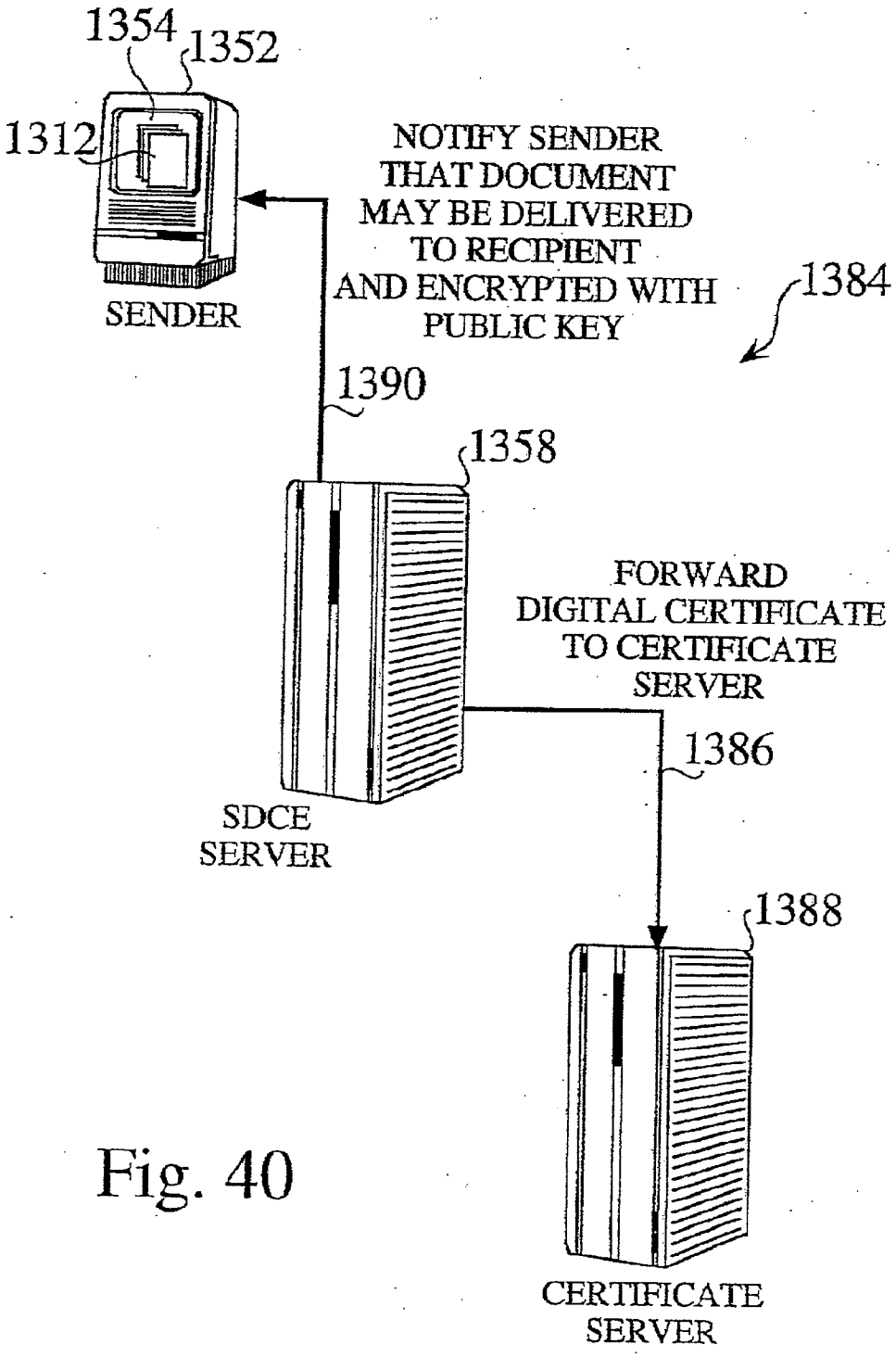

1354
1352
1312
SENDER
NOTIFY SENDER THAT DOCUMENT MAY BE DELIVERED TO RECIPIENT AND ENCRYPTED WITH PUBLIC KEY
1384
1390
1358
FORWARD DIGITAL CERTIFICATE TO CERTIFICATE SERVER
1386
SDCE SERVER
1388
CERTIFICATE SERVER

Fig. 40

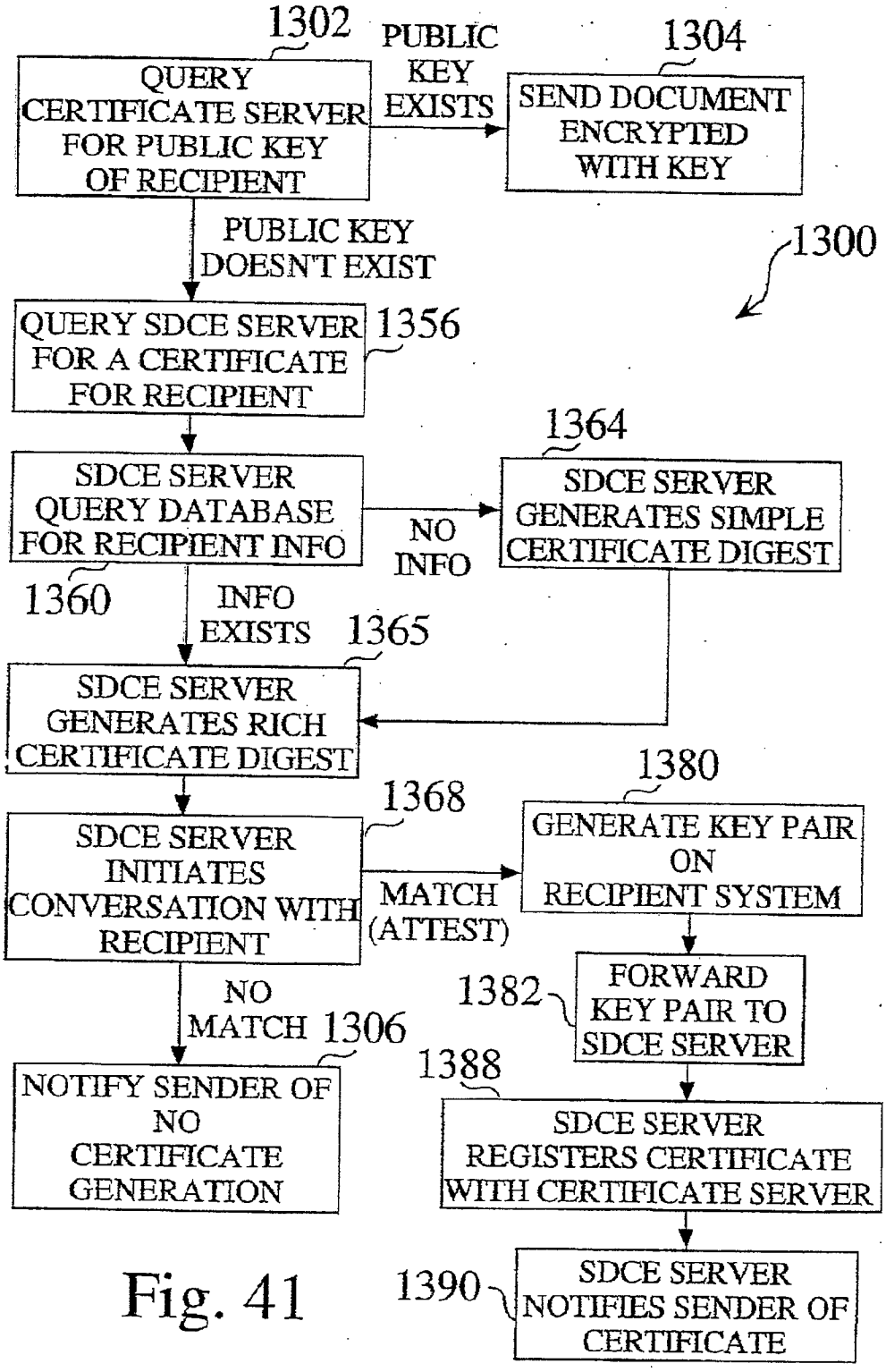

1302
QUERY CERTIFICATE SERVER FOR PUBLIC KEY OF RECIPIENT
PUBLIC KEY EXISTS
1304
SEND DOCUMENT ENCRYPTED WITH KEY
PUBLIC KEY DOESN'T EXIST
1300
QUERY SDCE SERVER FOR A CERTIFICATE FOR RECIPIENT
1356
1364
SDCE SERVER QUERY DATABASE FOR RECIPIENT INFO
NO INFO
SDCE SERVER GENERATES SIMPLE CERTIFICATE DIGEST
1360
INFO EXISTS
1365
SDCE SERVER GENERATES RICH CERTIFICATE DIGEST
1380
1368
SDCE SERVER INITIATES CONVERSATION WITH RECIPIENT
MATCH (ATTEST)
GENERATE KEY PAIR ON RECIPIENT SYSTEM
1382
FORWARD KEY PAIR TO SDCE SERVER
NO MATCH
1306
1388
NOTIFY SENDER OF NO CERTIFICATE GENERATION
SDCE SERVER REGISTERS CERTIFICATE WITH CERTIFICATE SERVER
1390
SDCE SERVER NOTIFIES SENDER OF CERTIFICATE

Fig. 41

ABSTRACT

A method and apparatus are provided for securely delivering documents over an electronic network while preserving document formatting. The invention also provides security that restricts access to the system to an authorized user. A document is sent from a sending computer to a dedicated server, using a send client application. The document is specified for delivery within the send client application, or by clicking and dragging the document onto an appropriate window or icon on the sending computer desktop, or is specified from within a document authoring application. A dedicated server stores the document and forwards an electronic notification to a receiving device. The stored document is downloaded from the dedicated server, using a receive client application, in response to the notification. The receive client application permits the recipient to receive, view, print, and/or manipulate the document. The dedicated server is preferably managed by a configuration user interface having an HTML interface for sending, tracking, accessing account information, managing billings, and managing mail distribution lists. The send client application allows a user to specify document delivery parameters. The parameters may be stored for later modification and/or use. A sender driven certificate enrollment system and methods of its use are also provided, in which a sender controls the generation of a digital certificate that is used to encrypt and send a document to a recipient in a secure manner. The sender compares previously stored recipient information to gathered information from the recipient. If the information matches, the sender transfers key generation software to the recipient, which produces the digital certificate, comprising a public and private key pair. The sender can then use the public key to encrypt and send the document to the recipient, wherein the recipient can use the matching private key to decrypt the document.